Deutschland Altermedia.info
www.altermedia-deutschland.info
In einer Zeit des Universalbetruges ist die Wahrheit zu sagen eine revolutionäre Tat (George Orwell)

SICHERHEITSHINWEISE FÜR NATIONALISTEN

Verfasser: http://sicherheit.nw.am
Bereitgestellt als PDF: http://altermedia-deutschland.info

TOR NETZWERK

Quelle: http://sicherheit.nw.am

Tor ist ein kostenloses *Netzwerk* zur *Anonymisierung* von *Verbindungsdaten*. Es wird für TCP-Verbindungen eingesetzt und kann beispielsweise für Web-Browsing, Instant Messaging, IRC, SSH, E-Mail, P2P und anderes benutzt werden. Tor schützt seine Nutzer vor der Analyse des Datenverkehrs.

I N H A L T S V E R Z E I C H N I S

- **Das Funtionsprinzip von TOR**
  - Grundlegendes
  - Hat die Polizei TOR unterwandert?
  - Wie funktioniert das Internet
  - Wie schützt TOR jetzt meine Daten?
- **Wie sicher und anonym ist TOR?**
  - Grundlegendes zu Sicherheit und Anonymität
  - Darauf weisen die Betreiber hin
- **Das richtige Paket – Installation und Inbetriebnahme**
  - Vorgehensweise
  - Das Tor-Paket enthält
  - Der Start
- **Torbrowser richtig einstellen**
  - Die Anleitung
- **Spezielle Torbrowser**
  - Welchen Browser sollte man benutzen?
- **Das TOR-Netzwerk alleine reicht nicht**
  - Wie kann ich mich weiter anonymisieren?
  - Der richtige Umgang mit Cookies
  - Der Schutz vor Spionageprogrammen (Spyware)
  - Die Absicherung deines Computers
  - Schutz deines W-LAN
  - Hintergrundwissen über die staatliche Vorratsdatenspeicherung
- **Anonymität und IP-Verschleierung testen**
  - Wogegen ich mich absichere
  - Feststellen der eigenen IP-Adresse
  - Aktiviere deinen Proxy
- **Verschiedene Hilfsprogramme**
  - Der CCleaner
  - Ad – Aware
  - Truecrypt unter Linux
  - Truecrypt unter Windows
- **Passwörter**
  - Passwortwahl
  - KeePass Password Safe

Das Funktionsprinzip von TOR

Bestimmt werden sich Laien fragen, wie das TOR Netzwerk ganze genau funktioniert. Das ist aber nicht weiter schlimm, es ist schließlich noch kein Meister vom Himmel gefallen.

Das Prinzip von TOR ist dermaßen kompliziert, dass es gar nicht darzustellen ist. Das was wir zeigen und die meisten kennen, ist ein vereinfachtes Schaubild. Es geht nur darum zu zeigen, was TOR mit unserer IP und unseren Daten macht, andere Verbindungsmöglichkeiten/-arten und die Prozesse im Hintergrund wären hier zu komplex.

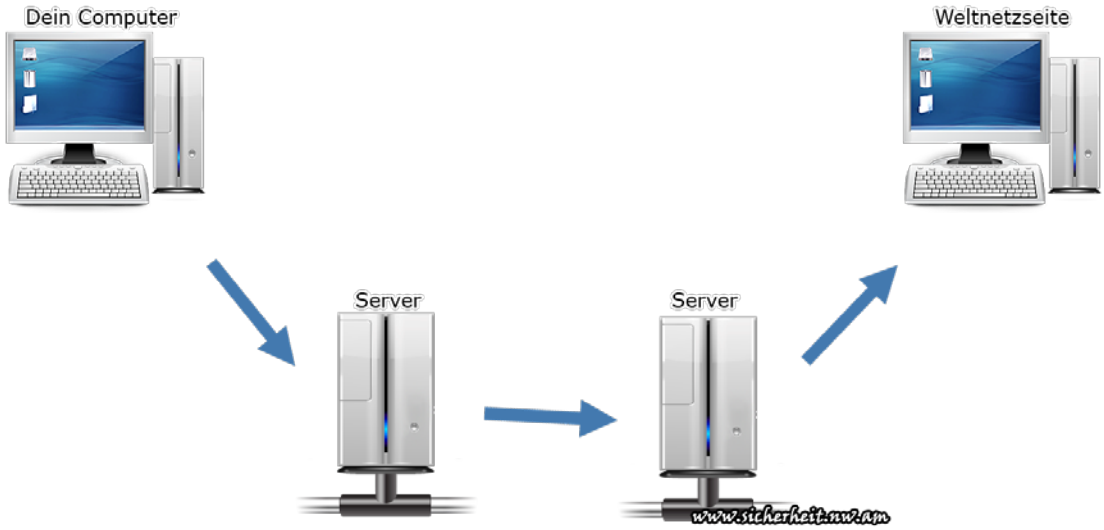
Außerdem weisen wir nochmals darauf hin, dass Tor keine Wunderwaffe ist. Die Schaubilder wurden vereinfacht und berücksichtigen nicht die falschen Einstellungen vieler Browser oder mögliche Polizeicomputer im TOR-Netzwerk

Hat die Polizei TOR unterwandert?

Nein, natürlich hat die Polizei auch eigene Rechner und Server mit dem TOR-Netzwerk verbunden. Allerdings sind solche Überwachungsmethoden fast vollkommen wirkungslos. Um das TOR-Netzwerk effektiv überwachen zu können, müsste die Polizei mindestens 40% des Netzwerkes unter ihrer Kontrolle haben. Praktisch unmöglich bei den Ressourcen der Deutschen Polizei.

Wie funktioniert das Internet?

Wir haben unseren Rechner der ins Internet geht. Über unseren Internetanbieter (T-Online z.B.) werden wir über ein paar Server zu der gewünschten Internetseite verbunden (grob vereinfacht).

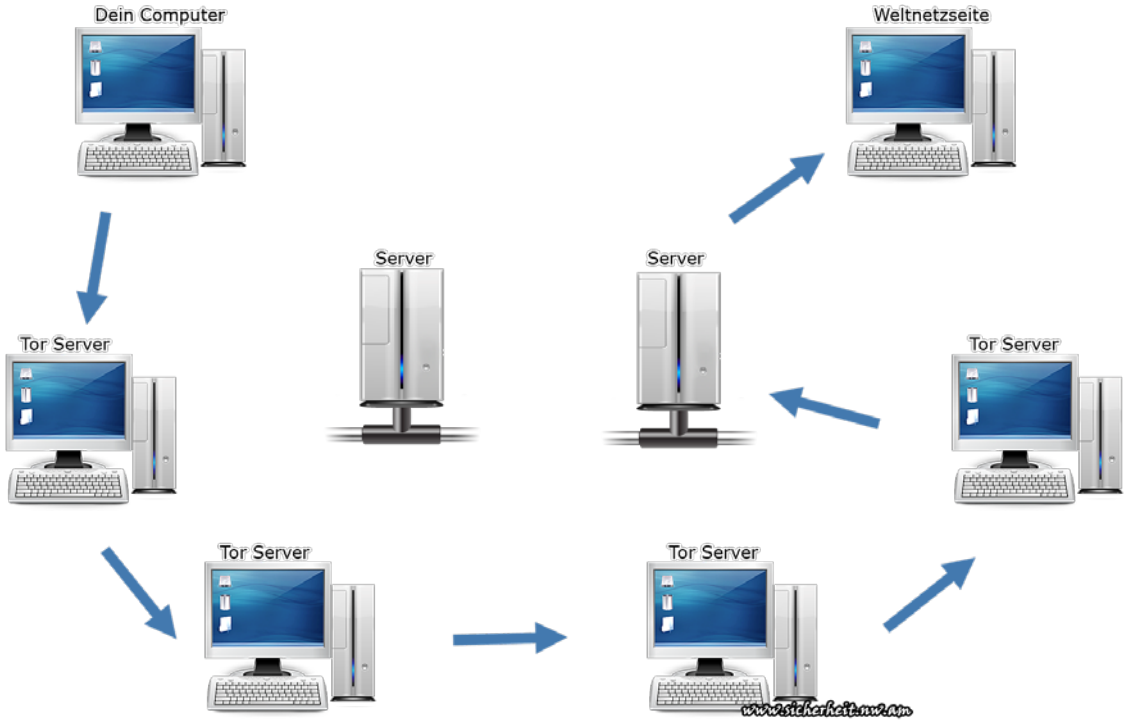


Ohne einen Proxy werden unsere Daten aber direkt an die Website weitergeleitet (IP etc.). Wenn jemand, z.B. die Polizei, also jetzt herausfinden möchte, wer auf die Website zugegriffen hat, fragt er bei der Website nach der IP.

Mit der IP geht die Polizei zu T-Online und fragt dort wieder nach, welcher Anschluss zu einer bestimmten Zeit mit dieser IP unterwegs war. Der Anbieter gibt die Daten heraus und schon weiß die Polizei, dass wir diese Seite besucht haben.

Wie schützt TOR jetzt meine Daten?

Sobald TOR oder ein anderer Proxy installiert wurde, geht man nur noch über diese Software ins Internet. Niemals über den normalen Browser ins Internet gehen und glauben TOR würde schon alles Regeln! Durch einen Proxy entsteht folgende Verbindung (vereinfacht):



Unser Computer wird von TOR zu einem anderen Rechner weitergeleitet. User von TOR können ihren PC als Knotenpunkt zur Verfügung stellen; je mehr desto besser. Jeder Knotenpunkt sendet jetzt unsere Anfrage zum nächsten Knotenpunkt.

Dabei verwenden wir nicht mehr unsere IP, sondern eine der Knotenpunkte bzw. die des letzten Knotenpunktes. Denn der letzte Knotenpunkt (Ausgang) greift auf den Server der Website zu. Die Website sieht also nur die IP des Ausgangs, unsere bleibt verborgen.

So funktioniert TOR!

Wie sicher und anonym ist TOR?

Tor ermöglicht es Benutzern, ihren Aufenthaltsort zu verbergen, während sie verschiedene Dienste wie z.B. Veröffentlichungen im Web oder Instant-Messaging verwenden.

Durch die Verwendung von Tor "Rendezvouspunkten" können andere Tor-Benutzer auf diese versteckten Dienste zugreifen, ohne dabei die Netzwerkidentität des Anderen zu kennen. Das Projekt TOR ist aber noch in der Entwicklungsphase. Wie effektiv man darüber im Internet surfen kann, hängt zudem von jeweiligen Nutzer selbst ab.

Darauf weisen auch die Betreiber hin:

> Tor kann nicht alle Anonymitätsprobleme lösen. Es konzentriert sich darauf, den Transport von Daten zu schützen.

Du musst protokollspezifische Software verwenden, wenn du nicht möchtest, dass die von dir besuchten Seiten, Informationen über deine Identität erhalten. Beispielsweise kannst du einen Webproxy wie Privoxy verwenden, um Cookies und die Herausgabe von Informationen über Ihren Browsertyp zu blockieren.

Das richtige Paket - Installation und Inbetriebnahme

TOR muss nicht mehr mühsam Schritt für Schritt installiert werden. Du musst nur die Datei runterladen, sie extrahieren (entpacken) und in dem nun neuen Ordner auf *Start Tor Browser* drücken.

Auf der Weltnetzseite von TOR gibt es zahlreiche Pakete von TOR. Von der Vielfalt sollte man sich aber nicht verunsichern lassen und sich an folgende Regeln halten:

- Das richtige Betriebssystem wählen
- Nur die stabilen Versionen runterladen
- Das TOR Bundle runterladen (auch "*Tor Browser Bundle*" genannt)

Am besten lädt man sich das Komplettpaket runter, und extrahiert es auf einen USB Stick. So kann man TOR an jedem Rechner benutzen ohne etwas neu installieren zu müssen

Das Tor Paket enthält:

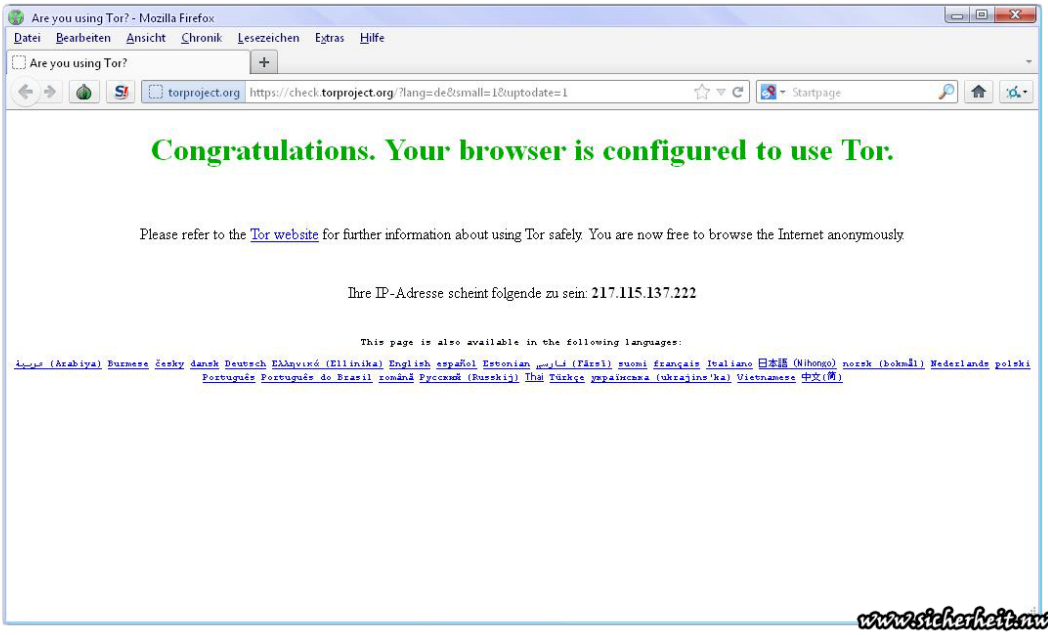
- Tor Software (portable)
- Firefox (portalble)
- Polipo
- Vidalia

Der Start:

Polipo und Vidalia sind Zusatzprogramme die den Datenverkehr noch sicherer und anonymer machen sollen. Gestartet wird das Ganze dann direkt vom USB-Stick.

Dazu im Startorder "Tor Browser" auf "***Start Tor Browser***" klicken. Es öffnet sich ein Fenster und Tor beginnt sofort mit dem Aufbau.

Sobald die Verbindung hergestellt ist, erscheint im Startfenster eine grüne Zwiebel und es öffnet sich nach wenigen Sekunden der Firefox Browser.


Are you using Tor? - Mozilla Firefox
Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
Are you using Tor?
torproject.org https://check.torproject.org/?lang=de&small=1&uptodate=1
Startpage
Congratulations. Your browser is configured to use Tor.
Please refer to the Tor website for further information about using Tor safely. You are now free to browse the Internet anonymously.
Ihre IP-Adresse scheint folgende zu sein: 217.115.137.222
This page is also available in the following languages:
(Arabiya) Burmese česky dansk Deutsch Ελληνικά (Ellinika) English español Estonian فارسی (Fārsī) suomi français Italiano 日本語 (Nihongo) norsk (bokmål) Nederlands polski
Português Português do Brasil română Русский (Russkij) Thai Türkçe українська (ukrajins'ka) Vietnamese 中文(簡)
www.sicherheit.nu.am

Siehst du diese Weltnetzseite in dem Browser ist er erfolgreich mit dem TOR Netzwerk verbunden und du kannst nun anonym durchs Weltnetz "surfen".

In den Einstellungen im Startmenü kann man TOR natürlich auch auf Deutsch umstellen!

Torbrowser richtig einstellen

Normalerweise sind Torbrowser und die Tor-Pakete schon richtig eingestellt. Wenn man allerdings seinen eigenen Browser verwenden will, muss man ihn noch richtig einstellen.

Anleitung:

1) Auf der Weltnetzseite von TOR lädt man sich das aktuellste "vidalia-bundle" herunter.

2) Dieses wird normal installiert.

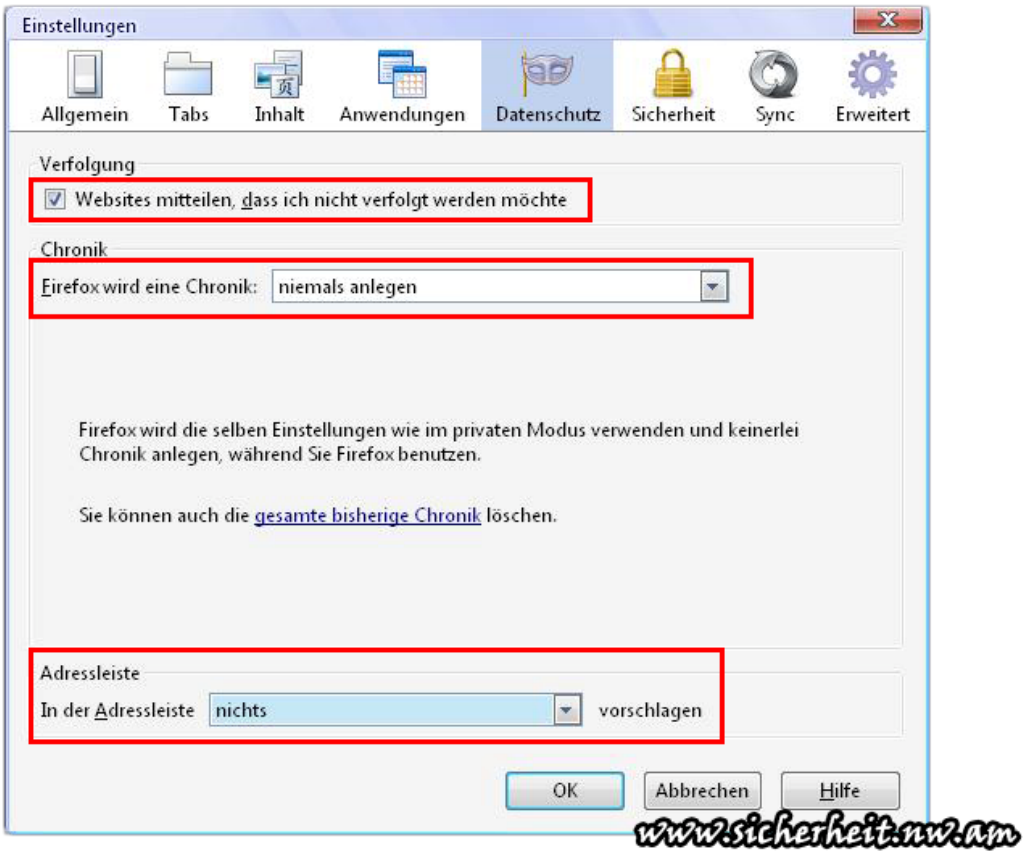
3) Jetzt muss man zuerst die Tor Software starten und eine Verbindung aufbauen lassen.

4) Beim Bundle kann es sein, dass jetzt der normale Browser startet. Wenn nicht, muss man ihn manuell starten. Rechts unten im Browser sollte der "Torbutton" zu sehen sein. Dieser sollte grün leuchten und "Tor läuft" anzeigen.

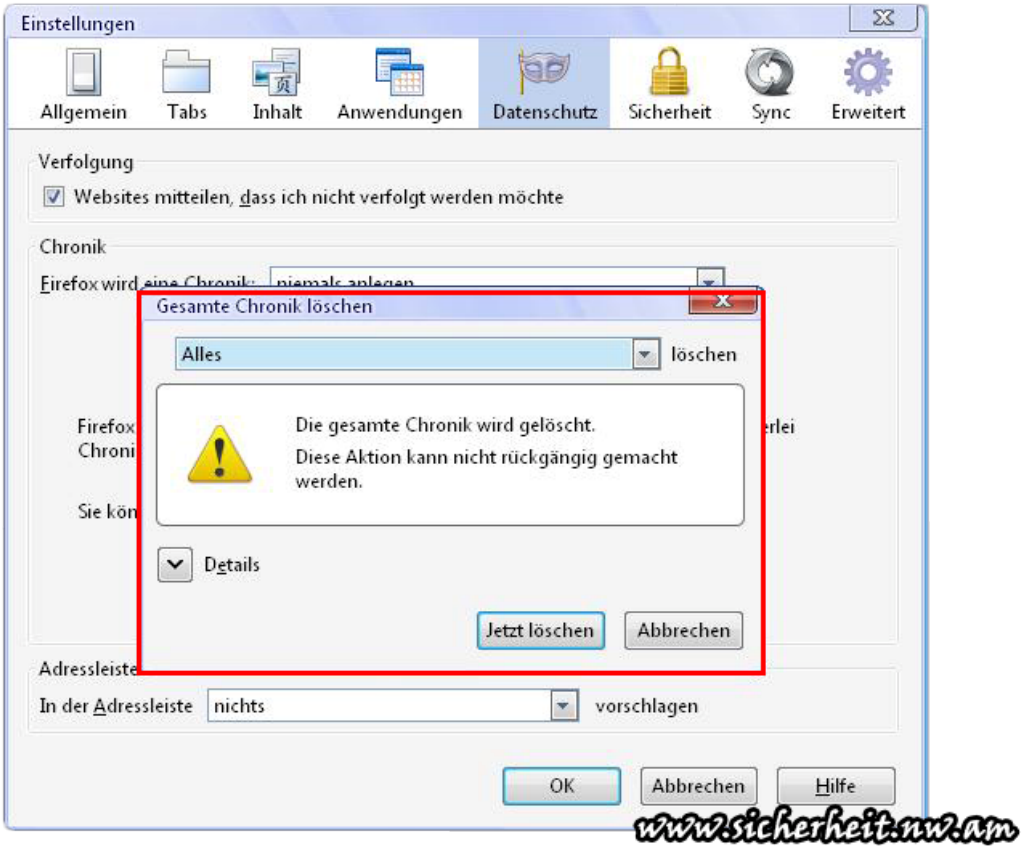
5) So, Tor läuft also, aber im Gegensatz zu den Portablen Firefox-Torbrowser oder den anderen Torbrowsern, ist unserer noch nicht richtig eingestellt (hier Firefox).

6) Zuerst muss man alle alten Cookies löschen. Dazu im Firefoxbrowser auf ***Extras*** > ***Einstellungen***, klicken.

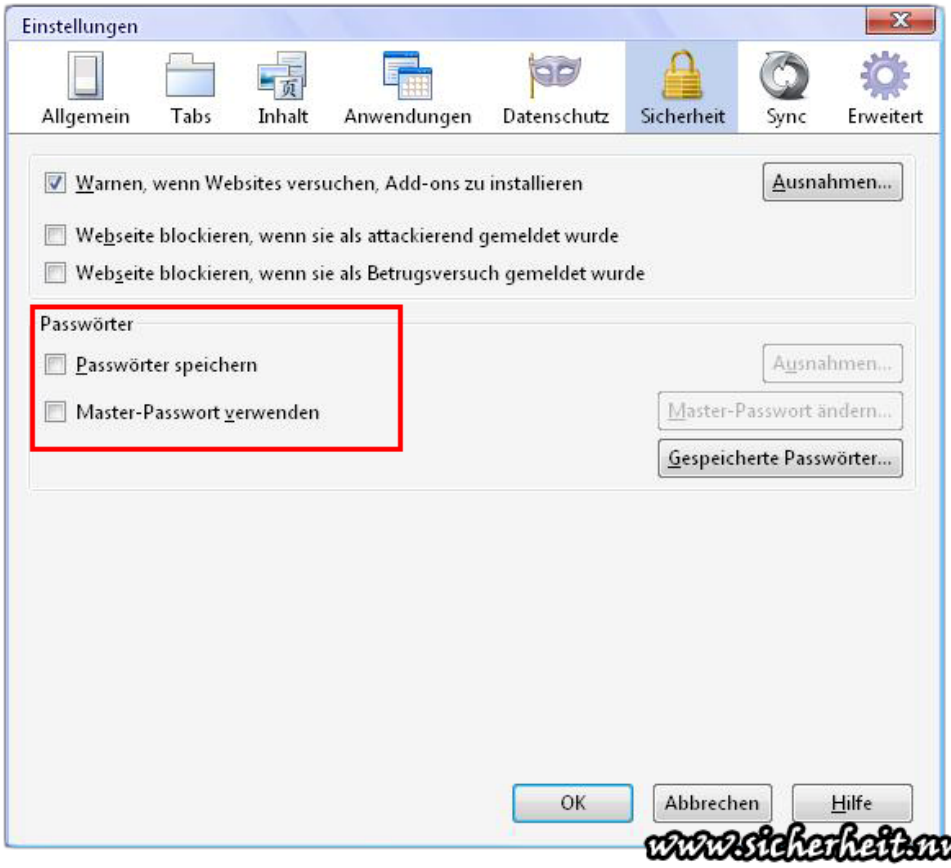
7) In der Registerkarte ***Datenschutz*** ändert man die Einstellung der Chronik auf ***niemals anlegen***.



7a) Zusätzlich klickt man im selben Fenster noch auf ***gesamte bisherige Chronik löschen***. Hier wählt man dann alle Punkte aus und bestätigt seine Entscheidung.

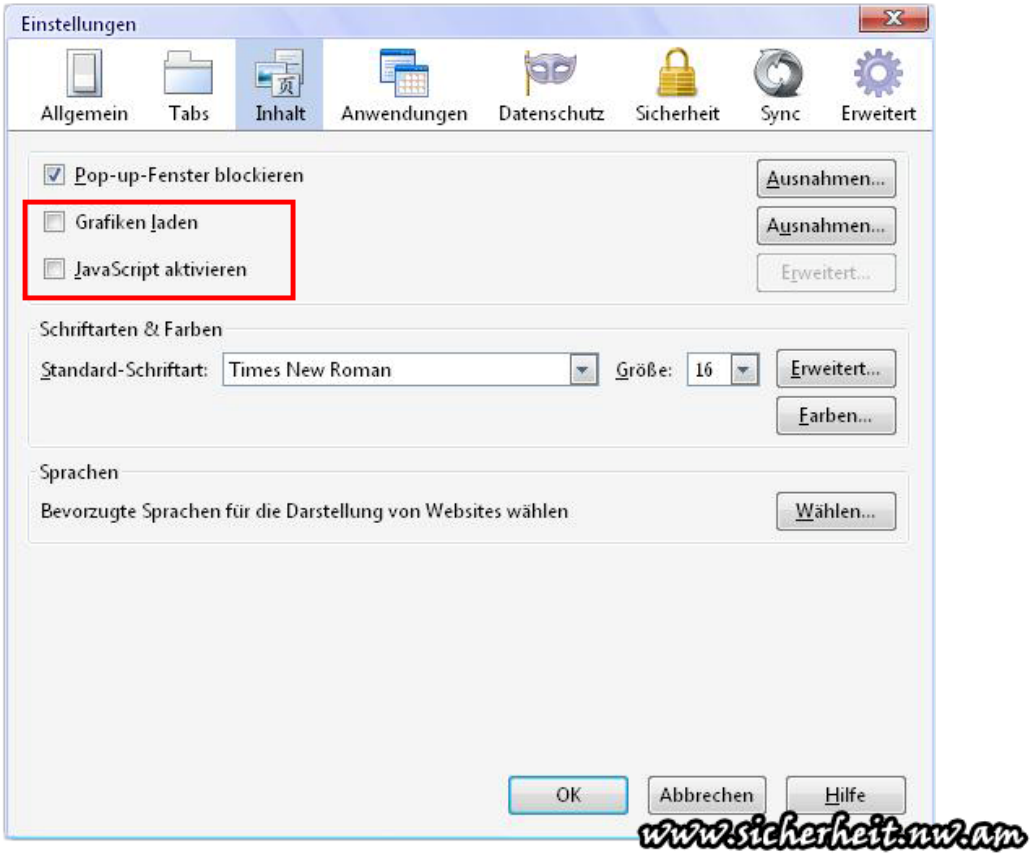


8) In der Registerkarte ***Sicherheit*** macht man die Haken bei ***Passwörter*** raus..



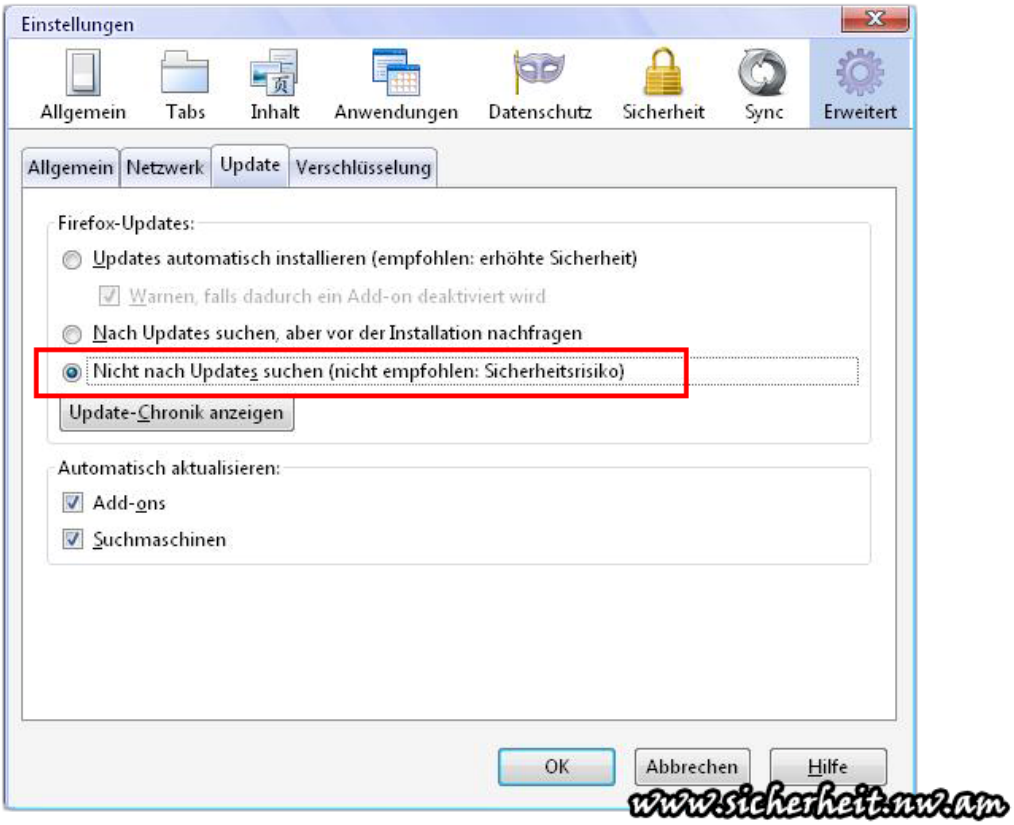
www.sicherheit.nw2.am

9) Jetzt hat man alle alten Spuren gelöscht. Aber das wichtigste kommt noch und zwar unter der Registerkarte ***Inhalt***.



10) Hier muss man die Punkte ***JavaScript laden*** und ***Grafiken laden*** deaktivieren. Wenn Java aktiviert bleibt, umgeht es einfach die Torsoftware und verrät unsere Daten an die Website.

11) Zuletzt muss man seinen Browser noch daran hindern, automatisch nach Updates zu suchen bzw. diese automatisch zu installieren. Diese Funktionen findet man in der Registerkarte ***Erweitert Update***



12) Alle Update Kästchen werden deaktiviert, alles mit ***OK*** abgesegnet und fertig.

Jetzt kann man ein wenig sicherer mit seinem alten Browser surfen!

Wir raten trotzdem dazu, Portable Torbrowser oder externe Torbrowser zu verwenden!

Spezielle Torbrowser

Wenn man TOR benutzen will, den Firefox aber nicht mag, kann man sich auch spezielle Torbrowser herunterladen.

Die bekanntesten sind die Opera Torbrowser und XeroBank. Diese Browser haben TOR schon mit installiert und sind auch schon perfekt eingestellt. Zudem verfügen sie über zahlreiche Tools die später im Hintergrund laufen und uns noch mehr Sicherheit verschaffen. Wir verwenden hier XeroBank.

XeroBank ist eigentlich Firefox, aber er sieht etwas anders aus!

Installation:

1. Man lädt sich den gewünschten Browser herunter, und installiert ihn ganz normal auf die Festplatte.

Bei XeroBank wählt man in der Installation statt ***XeroBank Client*** einfach ***Tor Version*** aus!

2. Jetzt startet man den Browser über das Icon. Es erscheint ein Ladebildschirm in dem klein *Connecting to Tor?* steht. Der Browser baut also selbstständig eine Verbindung zum TOR-Netzwerk auf.

2. Fertig, jetzt kann ganz normal weitergesurft werden.

Das TOR Netzwerk allein reicht nicht

Wenn du TOR nutzt, hast du schon Einiges für deine Anonymität im Weltnetz getan. Nur: Das reicht noch nicht. Du kannst nämlich trotzdem noch durch Dritte identifiziert werden. Das liegt daran, dass es neben der IP-Adresse noch andere Möglichkeiten gibt, beim Surfen mehr über dich zu erfahren. Zur echten Verschleierung deiner Identität im Weltnetz gehört:

(Ohne diese folgenden Schutzvorkehrungen nützt dir auch das TOR Netzwerk nichts - Du bist unter Umständen weiter identifizierbar.)

- **Der richtige Umgang mit Cookies**

Sei es am Arbeitsplatz, zuhause oder bei einem Bekannten:
Für neugierige Zeitgenossen ist es leicht ersichtlich, welche Adressen du im Internet aufgesucht hast; vorausgesetzt sie haben Zugriff auf den Rechner, an dem du vorher durchs Web gesurft bist: sie müssen nur wissen, an welchen Stellen sie nachzuschauen haben. Vor allem der Verlauf (die History), der Cache (Pufferspeicher, temporäre Internetdateien) und die Cookies geben Aufschluss über deine Surfgewohnheiten.
Vergessen solltest du natürlich auch nicht die Bookmarks (Lesezeichen, Favoriten), falls du dort Adressen gespeichert hat, die nicht für fremde Augen bestimmt sind!

Natürlich ist es aber hier möglich diese Spuren zu verwischen.

Das Programm **CCleaner** entfernt vor allem den Verlauf von besuchten Webseiten und diverse andere Verläufe, wie z.B. zuletzt benutzte Dateien oder eingegebene Suchbegriffe der Windows-Suche. Es ist auch möglich, unbenutzte und temporäre Dateien zu bereinigen. Erklärungen zu CCleaner erfolgen weiter unten in dieser Erklärung.

- **Schutz vor Spionage- und Werbesoftware ("Spy- und Adware")**

Neben der Gefahr von Viren, Würmern, Trojanern und den menschlichen Hackern an sich, gibt es auch noch die Bedrohung durch Werbe-(Adware) und Spionagesoftware (Spyware). Während ersteres, ausgeschrieben *„Advertising ware“ Werbungsprogramme*, eher harmlos aber sehr nervig ist, solltest du letzteres doch ernster nehmen, denn dabei geht es konkret um die Spionage deiner Daten.

Durch installierte Spy- oder Adware öffnen sich aus dem Nichts sogenannte *Popups*, kleine Internet-Explorer Fenster (da dieser integrierter Bestandteil von Microsoft Windows ist), die eben Werbung für Pokerfreunde, Finanz- oder Potenzschwache oder eben deine Vorlieben oder Schwächen anzeigt. Möglich ist auch, dass die ungewollt installierten Programme sich eben nicht bemerkbar machen und lediglich im Hintergrund Daten an einen anderen fest bestimmten Rechner senden.

Diese Art von Programmen dient dazu, dein Verhalten im Netz zu protokollieren, die Daten später weiterzugeben um sie kommerziell nutzen zu können und entweder durch gezielte Werbung oder sonstige Zwecke zu verarbeiten.

Doch es gibt natürlich Abhilfe in Form *Ad-Aware* von *Lavasoft*, zu welcher weiter unten die Installationsanleitung gezeigt wird.

- **Echtzeitverschlüsselung von Datenträgern**

Gerade im Falle einer Hausdurchsuchung ist es von enormem Vorteil, wenn der gesamte Rechner bzw. die gesamte Festplatte verschlüsselt ist.

Mit dem Programm *TrueCrypt* ist dies zum Beispiel möglich. Man wird nach dem Start des Rechners aufgefordert ein Passwort einzugeben und kann dann erst das Betriebssystem starten.

Ist der Rechner ausgeschaltet, ist die komplette Festplatte mit einem bestimmten Algorithmus verschlüsselt und kann somit nicht von Behörden oder anderen Schnüfflern eingesehen werden. Desweiteren bietet eine Vollverschlüsselung Schutz bei eventuellem Diebstahl des Notebooks.

Anzumerken ist, dass wenn eine neue Version des Programms erscheint, man den verschlüsselten Rechner mit der alten Programmversion natürlich weiterhin nutzen kann. Empfehlenswert ist es dennoch, den Rechner bei Eintreten eines solchen Falls, wieder komplett zu entschlüsseln und anschließend die neue Version zu installieren, mit welcher man den Rechner dann erneut komplett verschlüsselt.

Weiter unten folgen Anleitungen zu Truecrypt unter Linux und Windows.

- **WLAN Router - So schützt du dein Funknetz**

WLAN (Wireless Local Area Network, zu Deutsch: WLAN, drahtloses, lokales Netzwerk) galt noch vor wenigen Jahren als Thema für Technikspezialisten. Das hat sich geändert. Immer mehr Menschen schätzen die Vorteile des mobilen Internets. Ob in Cafes, im Hotel oder zuhause:

Ein WLAN-Router - genügt, um sich mit seinem Computer oder Laptop ins Internet einzubuchen.

Hier kannst du dich Informieren wie du deinWLAN-Router und dein Funknetz einrichtest und verschlüsselst.

WLAN, Router, Hotspot: Was ist das?

Ein WLAN ist nichts anderes als ein lokales Funknetz. Im Mittelpunkt steht dabei der so genannte Access-Point (AP), Hotspot oder Router, der mit dem Internet verbunden ist. Mit einem passenden Gerät kannst du dich in diesen Hotspot oder Access Point per Funk einbuchen und bekommst somit Zugang zum Internet. Die Reichweite der Funkverbindung hängt dabei von der eingesetzten Technik ab. In Gebäuden beträgt die Reichweite meist nicht mehr als 100 Meter. Im Freien und mit speziellen Antennen können durchaus mehrere Kilometer zwischen Access Point und Endgerät liegen. Der Standard, der WLAN möglich machte, wurde 1997 entwickelt.

Im Privathaushalt ist es in der Regel ein Router, der als Zugriffspunkt, dient. Dieser Router ist direkt mit dem Internet verbunden und sorgt über das Funknetz für die Anbindung der verschiedenen angeschlossenen Computer, etwa Laptops.

Gefahren bei WLAN

WLAN, sofern es ungesichert ist, lässt sich mit einer offenen Haustür vergleichen. Jeder, der in der Reichweite des Funknetzes ist, kann dieses mit entsprechender technischer Ausrüstung - einem so genannten *Sniffer* - aufspüren und sich Zugang zu deinem kabellosen Funknetz verschaffen. Und du als Betreiber des WLAN musst das nicht einmal merken.

Die Folgen:

- ☐ Zum einen könnten Unbefugte auf deine Kosten ins Internet gehen.
- ☐ Und noch schlimmer: Außenstehende könnten - ohne dass du es bemerkst auf deine persönlichen Daten zugreifen. Ob Urlaubsfotos, Zugang und Passworte zum Konto oder deine höchstpersönlichen Daten: Alles könnte der Unbekannte aus sicherer Entfernung sichten, herunterladen und dann gegen dich verwenden.

Kriminelle surfen mit - und du bist dran!

Letztlich, auch das ist schon vorgekommen, kannst du unter Umständen sogar für kriminelle Aktivitäten Dritter in Haftung genommen werden. Stelle dir vor, ein Außenstehender surft auf deine Kosten über dein WLAN, und ersteigert mit deinen persönlichen Daten bei einem Internetauktionshaus kostspielige Waren. Oder er lädt sich illegal Musikstücke (mp3) oder Filme herunter. Oder: Ein Krimineller, gar ein Terrorist, nutzt dein WLAN, um sich mit Komplizen auszutauschen. Als Beispiel seien hier die islamistischen Terroristen genannt, die im Sommer 2007 in Deutschland mehrere Bombenanschläge verüben wollten. Auch sie kommunizierten über das Internet - indem sie sich in ungesicherte WLAN-Netze Dritter einbuchten und so kaum identifizierbar ihrer kriminellen Aktivitäten nachgingen.

Spätestens in solchen Fällen hast du ein großes Problem nur, weil du dein Wireless LAN nicht ausreichend abgesichert hast. Denn Polizei, Anwälte und Abmahner haben in diesen Fällen zunächst einmal nur eins: Die IP-Adresse des Täters. Und das ist, wenn Dritte über deinen Internetzugang kriminell wurden, ***DEINE*** IP-Adresse, bzw. die deines Routers. Abmahnung, Hausdurchsuchung oder Ermittlungsverfahren werden also zunächst einmal gegen dich gerichtet sein.

Urteile: WLAN muss abgesichert werden

Auch die deutschen Gerichte urteilen immer öfter, dass jeder WLAN-Besitzer sein Funknetz gegen unbefugte Zugriffe schützen muss, weil er sonst zum so genannten Mitstörer wird.

> "*Es ist einem Anschlussinhaber aber zuzumuten, zumindest Standardmaßnahmen zur Verschlüsselung des Netzwerks zu ergreifen; ansonsten verschafft er nämlich objektiv Dritten die Möglichkeit, sich hinter seiner Person zu verstecken und im Schutz der von ihm geschaffenen Anonymität ohne Angst vor Entdeckung ungestraft Urheberrechtsverletzungen zu begehen (...)*"

stellte so das Landgericht Düsseldorf fest (Urteil vom 16.07.2008 - Az. 12 O 195/08).

Im Mai 2010 entschied dann auch der Bundesgerichtshof (BGH), dass private WLAN-Betreiber ihr Funknetz vor unberechtigten Zugriffen Dritter sichern müssen - durch eine angemessene Verschlüsselung und ein sicheres Passwort. Geschieht dies nicht, kann der WLAN-Betreiber im Fall von Urheberrechtsverletzungen Dritter abgemahnt werden und muss die entsprechenden Kosten zahlen.

WLAN-Schutz: Richtig einrichten

Dass sich viele WLAN-Besitzer in Gefahr begeben, liegt oft genug allein an reiner Bequemlichkeit. Man belässt es nach dem Kauf eines Systems einfach bei den Standardeinstellungen, die der Hersteller des WLAN vorgegeben hat - und vergisst dabei, dass diese Einstellungen eher auf Bedienungsfreundlichkeit, als auf Sicherheit ausgerichtet sind. Dabei lassen sich die Risiken mit wenigen Handgriffen und Einstellungen am Router und an den Endgeräten deutlich verringern:

- **Ändere** an deinem Router die eingetragene **SSID** (SSID = Service Set Identifier) und die Kennwörter für deine Netzwerkgeräte. Diese werden nämlich von den Herstellern mit Standard-SSID und -Kennwörtern ausgeliefert. Sie sind damit natürlich auf allen ausgelieferten Geräten gleich, und damit auch Hackern bekannt. Als SSID sollte immer eine schwer zu erratende Kombination von Ziffern und Buchstaben gewählt werden. Wer seine SSID in "Heim-Netzwerk" und "Stefan Müller" umtauft, kann die Änderung gleich bleiben lassen - eine willkürliche Kombination nach Art von "8BrLk45awe" ist weitaus sicherer. Um sich die Kombination zu merken, kann eine Eselsbrücke gute Dienste leisten.
  Beachte hierzu auch die Kapitel Passwortwahl.

- **Beschränke die MAC-Adressen.** Erlaube nur deinen eigenen Rechnern Zugriff auf den Access Point. Das lässt sich über die so genannten MAC-Adressen (MAC = Media Access Control) festlegen. Dafür trägst du die MAC-Adresse jedes von deinen verwendeten Computern oder Notebooks in den Access Point (Router) ein. Diese Adresse ist in der Netzwerkkarte gespeichert. Du ermittelst die Nummer mit dem Befehlszeilen-Tool **Ipconfig.EXE** (*Start -> Ausführen -> CMD -> Ipconfig*).
  Wenn du die Adressen eingetragen hast, und ein fremder Computer versucht, sich in dein Funknetz einzubuchen, wird er wegen der nicht übereinstimmenden Adresse abgewiesen.

- **Verschlüssel deine Kommunikation.** Wenn du den Zugriff auf dein Netzwerk nur auf bestimmte MAC-Adressen beschränkst, und eine deinem lokalen Funknetz eine schwer zu erratende SSID gegeben hast, bist du auf dem Weg zu mehr Sicherheit schon einen guten Schritt weiter. Dennoch ist der eigentliche Datenverkehr zwischen deinem Router und den Endgeräten noch völlig unverschlüsselt und kann abgefangen werden. Aktuell ist der Algorithmus **WPA 2**. Dieser verringert die Geschwindigkeit deines Funknetzes zwar ein wenig, doch dafür kann niemand mehr mitlesen, was du im Internet tust.
- **Schalte die Fernkonfiguration (Remote Management) ab.** Fernkonfiguration ist eine feine Sache, wenn man sie braucht. Doch auch Unbefugte können dieses "Remote Management" für ihre Zwecke nutzen. Wenn du diese Funktion nicht benötigst, deaktiviere sie.

- **Überprüfe Reichweite und Standort des Access Points** (also des Routers).
  Beim ersten Start deines Funk-Netzwerks solltest du unbedingt die Reichweite und den Standort deines Access Points überprüfen. Gehe dazu mit deinem Notebook oder Organizer ruhig aus dem Haus, stelle fest, in welcher Entfernung du noch auf das Netzwerk zugreifen kannst.
  Spätestens dann solltest du bedenken:

    - So weit du von deinem Access Point entfernt sein kannst, so weit könnte auch ein Unbefugter entfernt sein - und sich trotzdem noch in dein Netzwerk einbuchen. Begrenze also die Reichweite deines Netzwerks so weit als möglich. Gegebenenfalls stelle den Access Point in der Wohnungsmitte auf.
- **Aktiviere das WLAN nur bei Bedarf** und keinesfalls dauerhaft. Bei praktisch allen moderneren Routern ist das **De-/Aktivieren des WLAN** einfach per Tastendruck möglich; diese Taster sind allerdings - etwa bei der Fritz!Box wie auch beim Speedport W700/701/900V - relativ gut versteckt. Beim Speedport (700, 701, 900, nicht aber bei den Vorgängern 500/501) ist der entsprechende Taster auf der Rückseite des Geräts zu finden. Bei den ersten Fritz!Boxen ist dazu stattdessen ein kurzer Telefoncode möglich. Bei älteren Routern ist das De-/Aktivieren nur über den (Um-)Weg des Routerkonfigurationsmenüs möglich.

Wenn du alle oben aufgeführten Schritte befolgst, hast du schon ein gutes Stück zu deiner Sicherheit im kabellosen Netzwerk geschaffen. Zugleich solltest du dich weiter auf dem Laufenden halten. Überprüfe regelmäßig, ob für dein Netzwerk neue Sicherheits-Updates vorliegen. Informiere dich, ob neue Sicherheits-Lücken aufgetaucht sind, und wie du dich, deine Privatsphäre, deine Daten und dein Geld schützen kannst.

Vorratsdatenspeicherung und staatliche Überwachung

Vorratsdatenspeicherung und staatliche Überwachung griffen und greifen massiv in die Bürgerrechte ein.

Am 9. November 2007 beschloss der Bundestag mit den Stimmen von CDU, CSU und SPD die Vorratsspeicherung in Deutschland. Bundesbürger konnten also seit 1. Januar 2008 nicht mehr unbesorgt miteinander kommunizieren.

Ob du telefonierst, jemanden eine eBrief schickst oder eine Kurzmitteilung (SMS) versendest - jeder Schritt wurde protokolliert und sechs Monate lang gespeichert, damit Ermittlungsbehörden sie bei Bedarf abfragen können.

Erst im März 2010 kippte das Bundesverfassungsgericht das umstrittene Gesetz - vorerst. Was das für dich bedeutet und wie du dich zumindest ein kleines bisschen Privatheit bewahren können, haben wir auf diesen Seiten für dich zusammengestellt.

Diese Daten wurden gespeichert

- **Telefonate über Festnetz**: Deine Rufnummer und die Nummer des Angerufenen. Zeitpunkt und Dauer der Verbindung, Telefonanbieter
- **Telefonate über Mobilfunk**: Deine Handynummer und die Handynummer deines Gesprächspartners. Zeitpunkt und Dauer der Verbindung. Funkzelle (=Ort), in der du dich während des Gesprächs aufgehalten hast. Funkzelle (=Ort), in der dein sich Gesprächspartner sich während des Gesprächs aufgehalten hat.
- **IP-Telefonie**: Zeitpunkt und Dauer der Verbindung, deine IP-Adresse und die IP-Adresse des Angerufenen
- **Versand von SMS**: Deine Mobilfunknummer und die Nummer des Empfängers. Zeitpunkt des SMS-Versands und Zeitpunkt des SMS-Empfangs. Funkzelle (=Ort), in der du dich zum Zeitpunkt des SMS-Versands befandest.
- **Versand von Fax**: Die Rufnummer des Absenders der Fax-Botschaft, die Rufnummer des Empfängers, Zeitpunkt und Dauer der Verbindung
- **Versand von E-Mail**: Bei Versand einer Mail die Kennung deines elektronischen Postfachs und deine IP-Adresse sowie die Kennung des elektronischen Postfachs jedes Empfängers deiner Nachricht. Beim Empfang einer Mail die Kennung des Mail-Postfachs des Absenders und des Empfängers der Nachricht sowie die IP-Adresse des Absenders. Wenn du auf ein Mail-Postfach zugreifst, die Kennung des Fachs und deine IP-Adresse
- **Verbindungen ins Internet**: Beginn und Ende jeder Verbindung zum Internet, zugewiesene IP-Adresse, eindeutige Anschlusskennung

Wer speichert die Verbindungsdaten - und wie lange?

Die Vorratsdatenspeicherung sah vor, dass die Datenberge von den Telefongesellschaften, den Internet-Providern und den Anbietern öffentlich zugänglicher Internetzugänge (etwa

HotSpots in Flughäfen und Bahnhöfen) gespeichert werden. Und das auf eine Dauer von sechs Monaten. Anschließend müssen die Daten binnen einer Frist von einem Monat gelöscht werden.

Wer durfte die gespeicherten Verbindungsdaten einsehen?

- Polizeidienststellen
- Staatsanwaltschaften
- Verfassungsschutzämter
- Bundesnachrichtendienst
- Militärischer Abschirmdienst

Welche Bestandsdaten werden gespeichert?

Anbieter von Festnetz-Telefonie, Mobilfunk (Handy) oder Internet-Telefonie haben unabhängig von der Vorratsdatenspeicherung folgende Bestandsdaten ihrer Kunden abzufragen und zu speichern:

- Rufnummern bzw. Mailadresse
- Name des Kunden
- Anschrift des Kunden
- Geburtsdatum des Kunden
- Datum des Vertragsbeginns
- ggf. Anschrift des Festnetzanschlusses

Zudem sind die Anbieter verpflichtet, auf Anfrage spezielle Daten ihrer Kunden herauszugeben. Dazu gehören unter anderem:

- dynamische (also von Fall zu Fall vergebene) IP-Adressen
- Passworte
- PIN und PUK

Ist das letzte Wort schon gesprochen?

Im März 2010 erklärte das Bundesverfassungsgericht die Vorratsdatenspeicherung in ihrer bis dahin geltenden Form für verfassungswidrig und nichtig. Alle bis dahin gespeicherten Daten müssten sofort gelöscht werden, so die Karlsruher Richter.

Ein grundsätzliches Verbot der Vorratsdatenspeicherung gab es allerdings nicht. Die Richter stellten nur fest, dass eine solche Massen-Speicherung nach klareren und verfassungsrechtlich korrekten Regeln erfolgen müsse. Die Bundesregierung kündigte folglich ein neues Gesetz an.

Der *Arbeitskreis Vorratsdatenspeicherung* informiert laufend über die aktuelle Entwicklung. Fragen zur Speicherung von Verkehrsdaten beantwortet daneben die *Bundesnetzagentur*.

Anonymität und IP-Verschleierung testen

Es gibt viele Gründe dafür, seine Spuren im Weltnetz zu verschleiern - angefangen von Bedenken hinsichtlich des Datenschutzes bis hin zu Vorsichtsmaßnahmen gegen Spionage durch unlautere Zeitgenossen oder Werbeindustrie. Ob du wirklich anonym über einen Proxy oder ein Proxy-Tool surfst, kannst du ganz einfach überprüfen. Auf dieser Seite zeigen wir dir, wie es geht und stellen dir weiter unten einen Praxistest zur Verfügung.

Stelle deine echte IP-Adresse fest

In den vorhergegangenen Kapiteln haben wir gezeigt, wie du bei jeder Internet-Session eine IP-Adresse, also eine einzigartige Hausnummer im Netz, zugeteilt bekommst. Anonymes Surfen bedeutet, dass du diese IP-Adresse mit den geeigneten Mitteln verschleierst, etwa durch einen anonymen Proxy oder durch einen Rewebber-Service.

Ob dir dies gelungen ist, stellst du einfach fest, indem du deine tatsächliche IP-Adresse mit derjenigen vergleichen, die dein Gegenüber im Weltnetz zu sehen bekommt. Sind beide IPs identisch, kansst du identifiziert werden. Sind sie unterschiedlich, hast du deine Spuren beim Surfen erfolgreich verschleiert.

Stelle nun zunächst einmal deine derzeitige IP-Adresse fest. Dazu musst du je nach deinem Betriebssystem etwas unterschiedlich vorgehen:

- Bei **Windows 9x**: Start ->Programme -> MS-DOS-Eingabeaufforderung. Gebe nun winipcfg ein. Drücke die Returntaste. Dann siehst du deine IP-Adresse.
- Bei **Windows NT**: Start ->Programme -> MS-DOS-Eingabeaufforderung. Gebe nun ipconfig ein. Drücken die Returntaste. Dann siehst du deine IP-Adresse.
- Ähnlich problemlos funktioniert das Herausfinden der eigenen IP-Adresse unter **Windows XP, Vista, 7**: Start ->Ausführen -> cmd. Nun öffnet sich ein schwarzes Fenster, die Eingabeaufforderung von Windows. Tippe hier einfach ipconfig /all ein. Nun siehst du alle Einstellungen, die mit deiner Verbindung zusammenhängen, eben auch deine derzeitige IP-Adresse.

- Wenn du sich nicht durch die Windows Befehle kämpfen möchtest kannst du auch ganz einfach auf die Weltnetzseite *www.wieistmeineip.de* schauen.

Aktiviere deinen Proxy

Nachdem du deine eigene IP-Adresse festgestellt hast, solltest du nun, sofern noch nicht geschehen, dein Proxy-Tool aktivieren oder deinen Browser so einstellen, dass du über einen anonymen Proxy-Server im Internet surfst.

Aktualisiere nun diese Seite, indem du auf deiner Tastatur die Taste **F5** drückst. Vergleiche nun deine notierte, echte IP-Adresse mit der nun angezeigten IP-Adresse.

Wenn die beiden Adressen unterschiedlich sind, hast du einen guten Schritt in Richtung Anonymität im Internet getan.

Weltnetz (Internet) Verläufe Löschen

Sei es am Arbeitsplatz, zuhause oder bei einem Bekannten:
Für neugierige Zeitgenossen ist es leicht ersichtlich, welche Adressen du im Internet aufgesucht hast; vorausgesetzt sie haben Zugriff auf den Rechner, an dem du vorher durchs Web gesurft bist: sie müssen nur wissen, an welchen Stellen sie nachzuschauen haben. Vor allem der Verlauf (die History), der Cache (Pufferspeicher, temporäre Internetdateien) und die Cookies geben Aufschluss über deine Surfgewohnheiten.
Vergessen solltest du natürlich auch nicht die Bookmarks (Lesezeichen, Favoriten), falls du dort Adressen gespeichert hat, die nicht für fremde Augen bestimmt sind!

Natürlich ist es aber hier möglich diese Spuren zu verwischen.

Das Programm **cCleaner** entfernt vor allem den Verlauf von besuchten Webseiten und diverse andere Verläufe, wie z.B. zuletzt benutzte Dateien oder eingegebene Suchbegriffe der Windows-Suche. Es ist auch möglich, unbenutzte und temporäre Dateien zu bereinigen.

Der CCleaner

Was wird vom cCleaner bereinigt?

Internet Explorer

- Temporäre Dateien, Verlauf, Cookies, Autovervollständigung, index.dat-Dateien.

Firefox

- Temporäre Dateien, Verlauf, Cookies, Download-Verlauf, Formulardaten.

Google Chrome

- Temporäre Dateien, Verlauf, Cookies, Download-Verlauf, Formulardaten.

Opera

- Temporäre Dateien, Verlauf, Cookies, Download-Verlauf.

Safari

- Temporäre Dateien, Verlauf, Cookies, Formulardaten.

Weitere unterstützte Browser

- K-Meleon, Rockmelt, Flock, Google Chrome Canary, Chromium, SeaMonkey, Chrome Plus, SRWare Iron, Pale Moon, Phoenix, Netscape Navigator, Avant und Maxthon.

Windows

- Papierkorb, zuletzt geöffnete Dokumente, Temporäre Dateien, Logdateien, Zwischenablage, DNS Cache, Fehlerberichterstattung, Speicherabbilder, Jumplisten.

Registrierungsreiniger

- Erweiterte Funktionen zum Entfernen von unbenutzten und alten Einträgen, Dateierweiterungen, ActiveX Controls, ClassIDs, ProgIDs, Deinstallationen, Bibliotheken, Schriften, Hilfedateien, Anwendungspfaden, Icons, ungültigen Verknüpfungen und mehr...

Anwendungen von Drittanbietern

- Entfernt temporäre Dateien und zuletzt benutzte Dateilisten (MRUs) von vielen Anwendungen wie Windows Media Player, eMule, Google Toolbar, Microsoft Office, Nero, Adobe Acrobat, WinRAR, WinAce, WinZip und vielen anderen...

Näheres zum CCleaner

Mythen und Klischees in der Informatik zu beseitigen, erinnert nicht selten an den Kampf von Don Quijote, wobei der Unterhaltungswert in einigen arg strapazierten Bereichen eher gen null tendiert und sich auch eine gewisse Ermüdung breit macht, wenn es darum geht, ständig den gleichen Unsinn zu revidieren. Das soll uns nicht davon abhalten, noch einmal das Thema Datenmüll-Bereinigung und Registry Cleaner aufzugreifen, um vielleicht doch noch etwas mehr Skepsis bei dem Umgang mit diesen Tools zu erzeugen.

Um es ganz deutlich zu formulieren, in diesem Artikel geht es nicht um die Vorzüge von Registry Cleanern, sondern in erster Linie um den CCleaner, den wir nach wie vor für als sehr nützlichen Helfer beim Eliminieren von Datenmüll einstufen. Das Thema **Registry Cleaner** reflektieren wir in einem extra Kapitel gegen Ende dieser Anleitung, zu der wir dir viel Vergnügen und hoffentlich die richtigen Erkenntnisse wünschen...

Hier gezeigte Programmversion: **v3.23.1823**

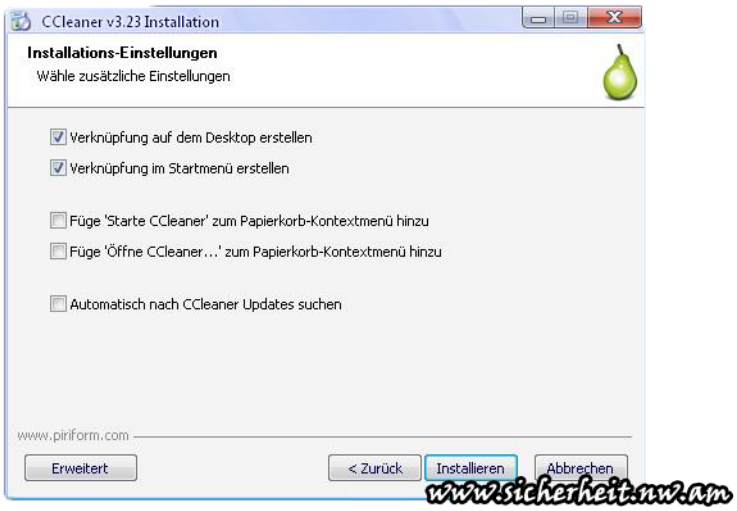
Installation und wichtige Hinweise:

Um in den Genuß des CCleaners zu kommen, benötigen wir natürlich den entsprechenden Download, eine 32 oder 64 bittige Unterscheidung gibts es weder für den Download noch für die Installation:

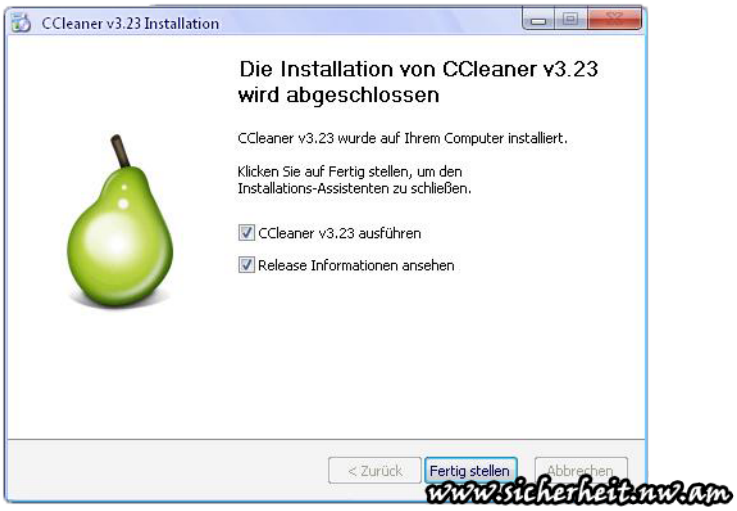
Nachdem wir die INSTALLATIONSDATEI heruntergeladen haben, öffnen wir sie mit einem Doppelklick.

Achte bei der Installation bitte darauf, das du überflüssige Zusatztools (speziell die Yahoo Toolbar oder Google Toolbar/Google Chrome) ***nicht*** mit installierst. Natürlich muß und will Piriform über dieses virale Marketing Geld verdienen, aber bitteschön nicht unbedingt gerade mit diesen Tools. Schließlich wollen wir die Datenmüllbeseitigung des CCleaners nicht dadurch konterkarieren, in dem wir quasi durch die Hintertür beispielsweise die Argusaugen des Suchmaschinen-Marktführers ins System zurückholen...

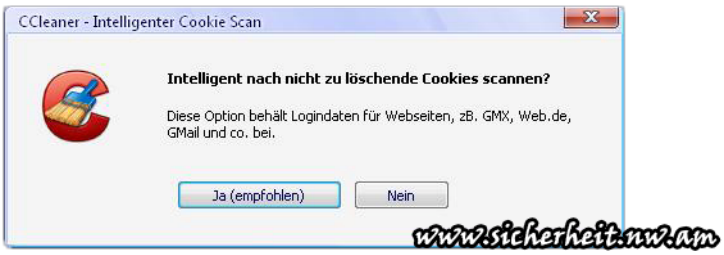
Während der Installation werden wir auch nach der Sprachversion gefragt, die du nach Gusto auswählen kannst, der CCleaner legt dir diesbezüglich kaum Steine in den Weg.



Auch die ganzen zusätzlichen Kontextmenüeinträge usw. sind absolut überflüssig (bitte den Screenshot beachten), weil sie nur zu Klicks verleiten, die eher an die Spontanität als Vernunft zu adressieren sind. Automatischen Updates sollte man grundsätzlich mit Skepsis gegenüberstehen, zumindest bei 3rd-party Software und zu denen gehört der CCleaner. Der Grund ist kausal, alles was in diesem Bereich aktiv ist, mischt sich in Systemressourcen ein, die nicht immer mit den hierarchischen Abfolgen eines Betriebssystems harmonieren !

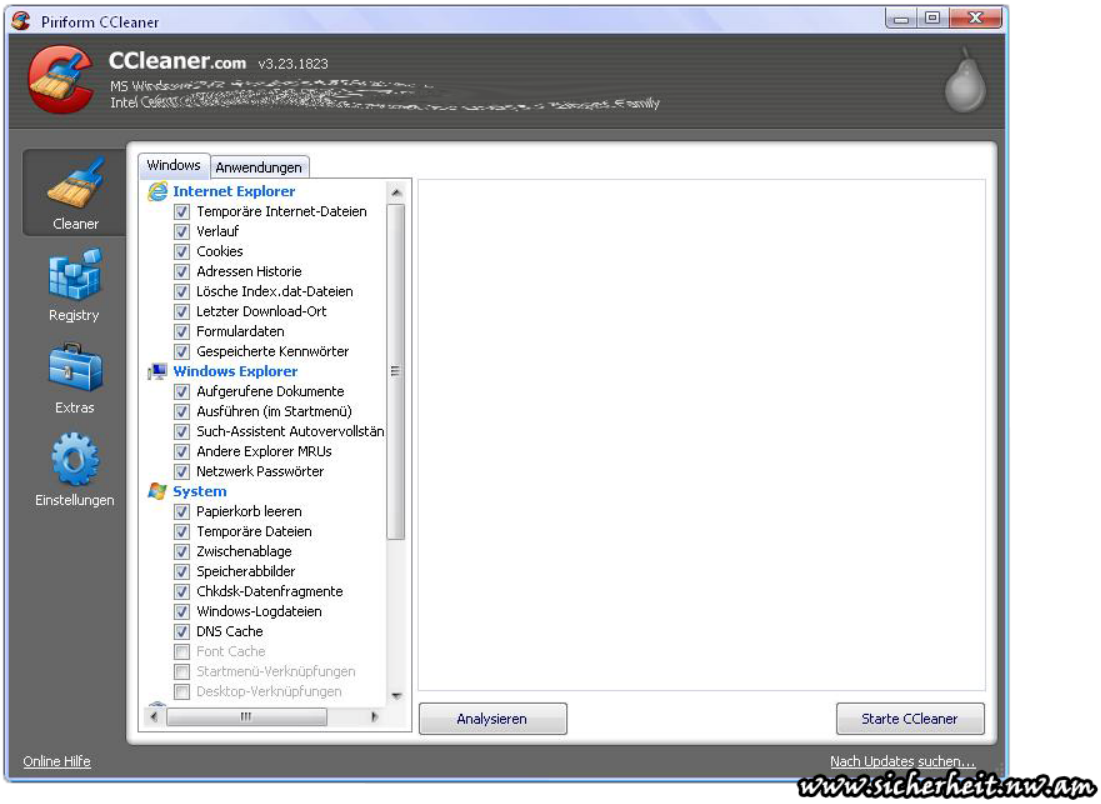


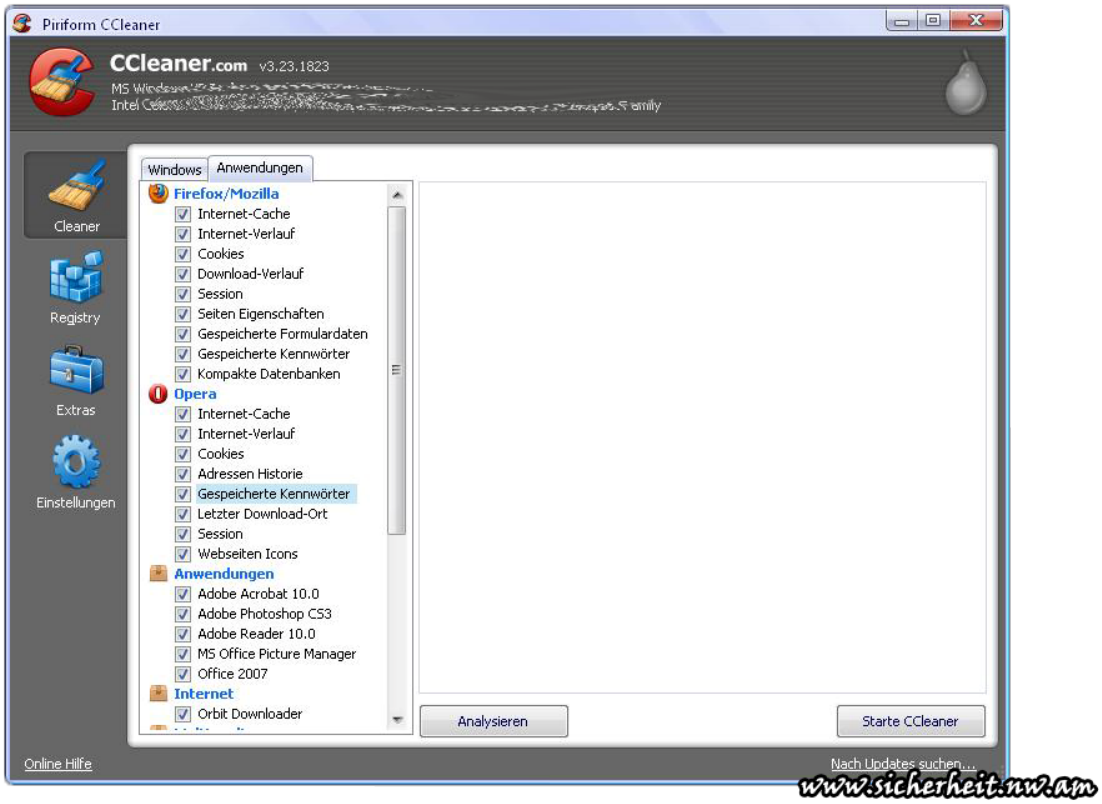
Beim klick auf **Fertig stellen** öffnet sich ein Fenster in dem du gefragt wirst ob du nach nicht zu löschenden Coocies scannen möchtest. Wir klicken hier natürlich auf **Ja**.


CCleaner - Intelligenter Cookie Scan
Intelligent nach nicht zu löschende Cookies scannen?
Diese Option behält Logindaten für Webseiten, zB. GMX, Web.de, GMail und co. bei.
Ja (empfohlen)
Nein
www.sicherheit.nw.am

Wichtige und gefahrlose Einstellungen:

Wenn die Installation absolviert wurde und du den CCleaner das erste mal mit Adminrechten startest, geht es an die Einstellungen des CCleaners, für die wir dir entsprechende Screenshots angefertigt haben, damit du die gefahrlosesten Einstellungen übernehmen kannst. Unsere Einstellungen basieren auf Langzeiterfahrungen mit den Betriebssystemen Windows XP ->Vista und Windows 7, wobei die aktuelle Windows 8 Preview sich bisher analog dazu verhält:





Die Begründung für diese Einstellungen liegen auf der Hand: **Kennwörter sollten grundsätzlich nie gespeichert werden**, egal in welchem Bereich sie angelegt wurden. Verknüpfungen werden von Windows Vista und auch Windows 7 anders kategorisiert als noch zu Zeiten von Windows XP, darum raten wir von deren Bereinigung ab. Dies gilt ebenso für tiefergreifende Systembereinigungen (**ausgegraute Bereiche**), bei denen schon eine zu viel gelöschte Datei ausreicht, um die ersten Probleme zu generieren.

Was im Karteireiter "**Anwendungen**" bereinigt werden kann, hängt natürlich in erster Linie davon ab, was du an externen Programmen installiert hast. Grundsätzlich sind diesbezüglich aber kaum Systemirritationen zu erwarten, zumindest nicht vom Betriebssystem. Darüber hinaus ist der CCleaner mittlerweilse so ausgereift, das diesbezüglich relativ wenig Substanz für Fehlerquellen existieren. Solltest du allerdings Software verwenden, die in dieser Hinsicht anfällig reagiert, kannst du jederzeit deren Optionshaken wieder entfernen.

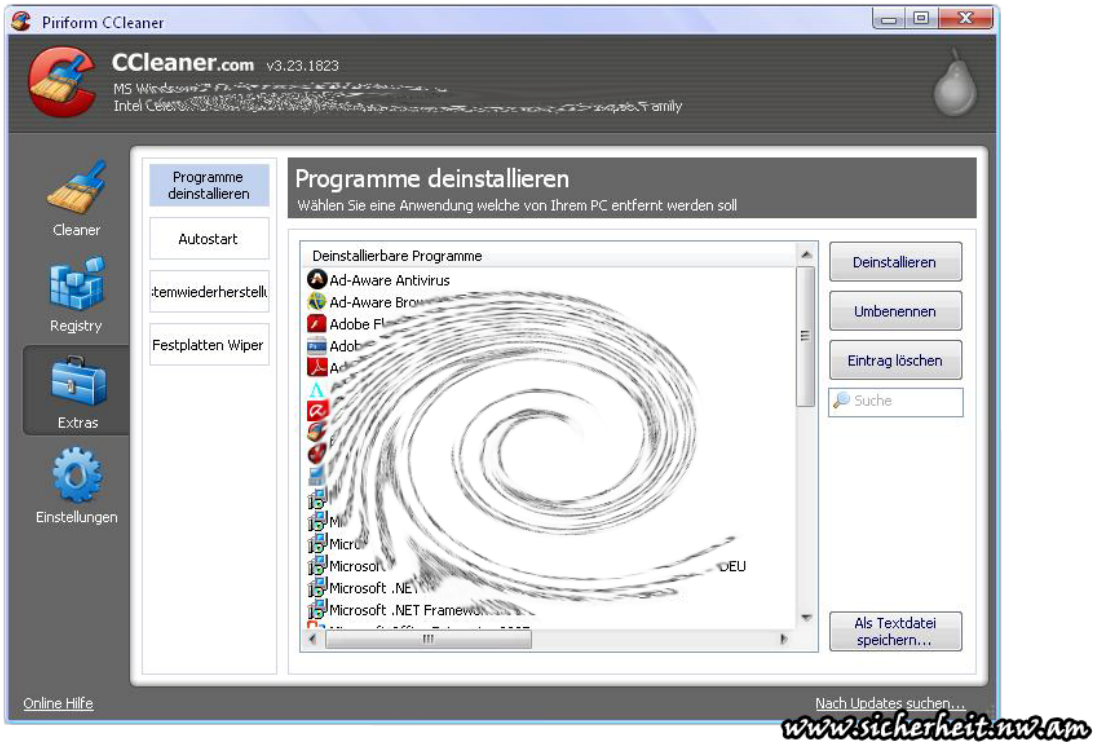
Kurzum: Über diese nun klar definierte Reinigungsroutine kannst du deinen Computer gefahrlos z.B. nach jeder Internetsitzung oder Programminstallationen bereinigen, ohne das du sensible systemrelevante Bereiche tangiert. Selbstverständlich kannst du unsere Vorgabe auch nach Gusto ändern, wir haben so allerdings die besten Erfahrungen gemacht und unsere Prämisse hieß: **möglichst gefahrlos und mit minimalem Risiko...!**

apropos Risiko:

Wir empfehlen ohnehin vor der ersten Systembereinigung mit dem CCleaner auf einem frisch

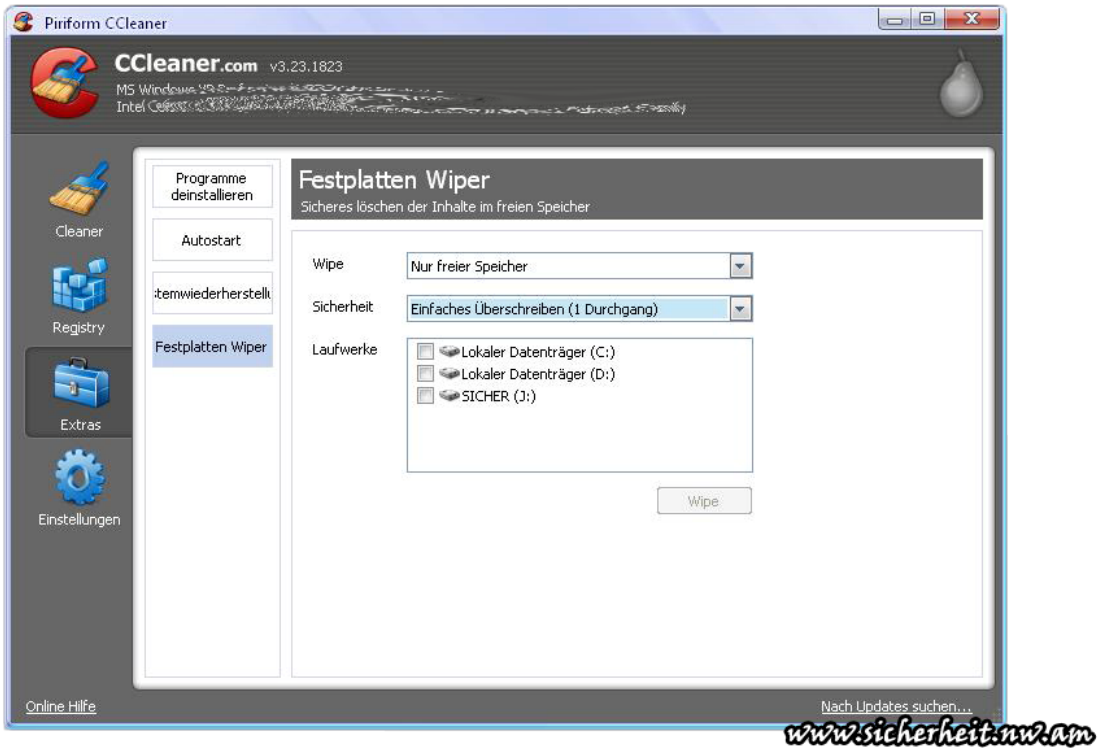
eingerichteten System ein Image (Abbild) mit einer geeigneten Software zu erzeugen, damit du immer einen passenden Rettungsanker parat hast.

Den Karteireiter **Registry** ignorieren wir ganz bewußt (warum steht im separaten Kapitel) und widmen uns dem nächsten interessanten Punkt: der Button **Extras**:

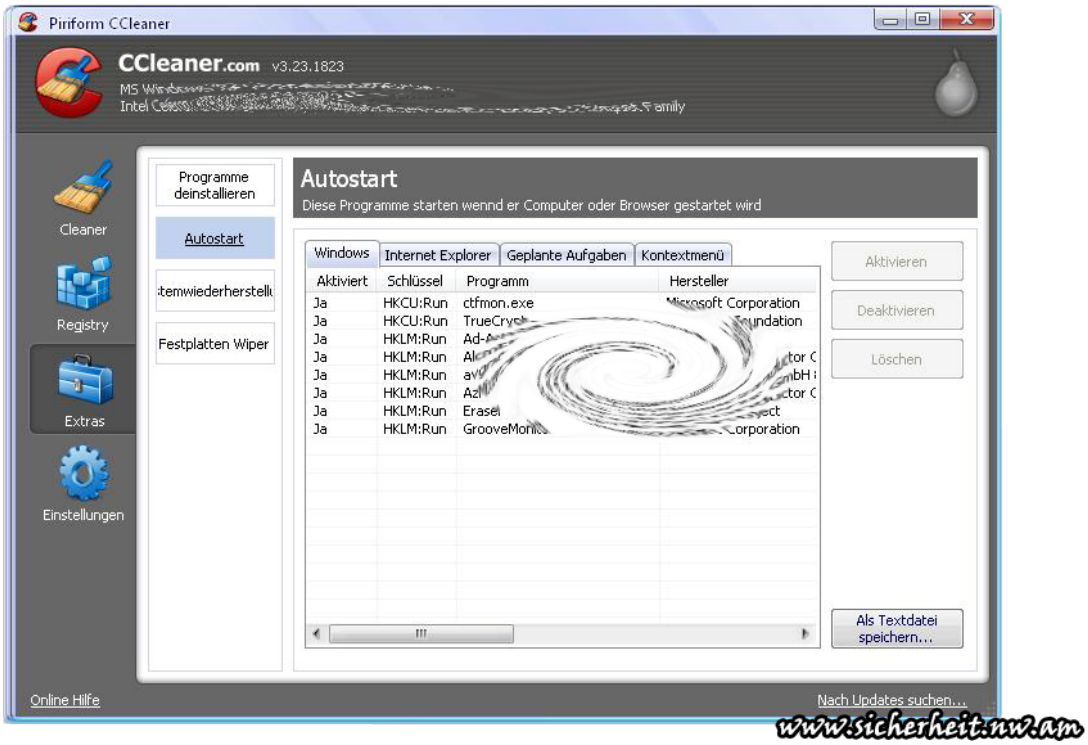


Hier finden wir insgesamt vier Untermenüs: Programme deinstallieren, Autostart, Systemwiederherstellung und Festplatten Wiper.

Programme lassen sich unter Windows Vista und Windows 7 mittlerweilse ausgezeichnet deinstallieren und falls nicht, hilft der CCleaner auch nicht entscheidend weiter, denn schlecht programmierte Deinstallationsroutinen lassen sich in der Regel von solchen Hilfsmaßnahmen wenig beeindrucken. Dies gilt ebenso für die Systemwiederherstellung, die ohnehin nur so gut funktioniert, wie Windows es zuläßt.

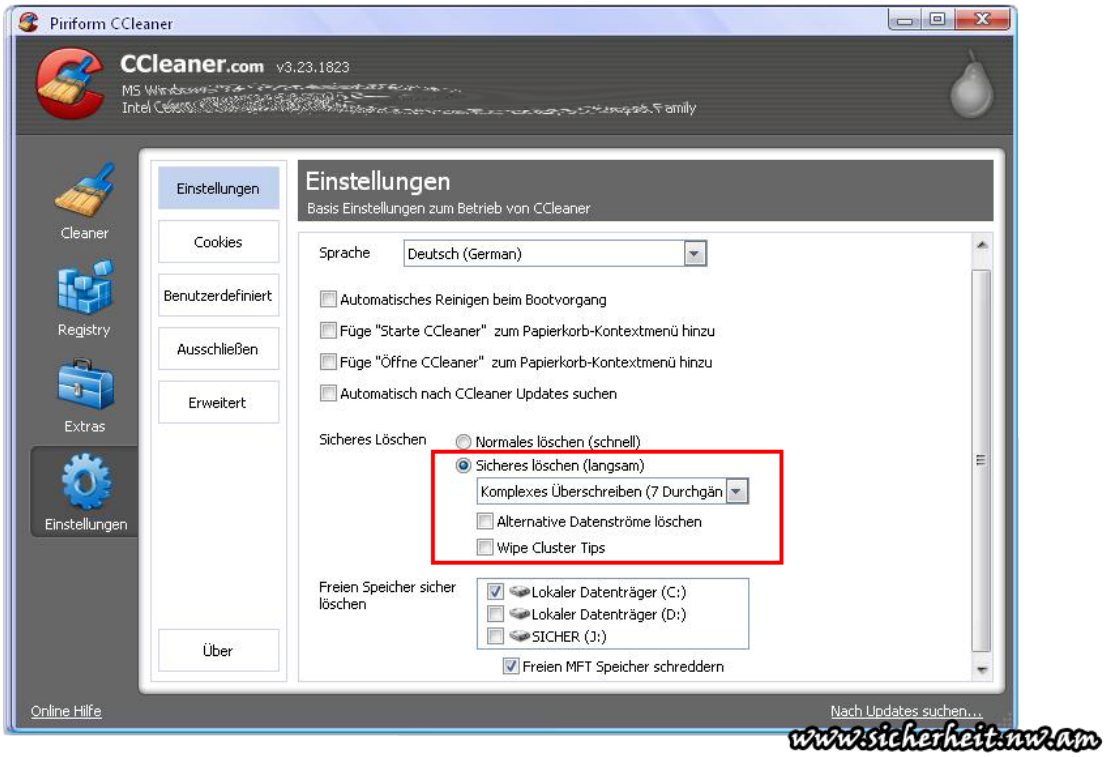


Festplatten Wiper (sicheres Löschen) von feierm Speicherplatz auf deinen Festplatten brauchen wir eigentlich nicht solange wir alle Daten sicher Löschen und nicht nur in den Papierkorb werfen. Bliebe noch der Punkt Autostart, der in der Tat durchaus einige Ansätze bietet, um gezielt ins System einzugreifen, wenn msconfig an seine Grenzen stößt:



Die Möglichkeit störende Einträge nicht gleich zu löschen, sondern zunächst zu deaktivieren und bei Bedarf wieder zu aktivieren, ist sicher einer der Vorzüge in diesem Abschnitt des CCleaners, zumal er neben dem Windows Autostart zusätzlich noch den Internet Explorer und Scheduled Tasks (geplante Aufgaben) als erweiterte Optionen anbietet, da kann msconfig nicht mithalten. Aber auch hier gilt wieder, Hände weg von der Maus, wenn du nicht weißt was diese oder jene Einstellung bewirkt und lösche bitte nicht gleich die Autostarteinträge ! sondern bleibe maximal bei der Deaktivierung.

Kommen wir zum Optionsbutton **Einstellungen**:



Unter Einstellungen -> Einstellungen achte bitte wieder darauf, dass du eine Optionen fürs sichere Löschen angehakt hast. Z.b.: Sicheres Löschen - Komplexes Überschreiben (7 Durchgänge).

Die Einstellungen der Cookies überlassen wir dir, diesbezüglich ist es kaum möglich, eine allgemeingültige Empfehlung abzubilden, dazu spielen in dieser Hinsicht zu viele verschiedene Faktoren eine Rolle. Wenn du aber der Meinung bist, das deine besuchten Weltnetzseiten keinerlei individuelle Surfgewohnheiten speichern sollten, kann die Konsequenz nur lauten: keine Ausnahmen in die Cookie Liste eintragen.

Willst du neben den standardmäßigen temporären Ordnern noch weitere bereinigen, so ist das über die Rubrik Benutzerdefiniert möglich. Eine Liste für mögliche temporäre Ordner (nicht alle sind auch zwangsweise vorhanden) unter Windows haben wir für kurz skizziert:

Windows XP:

C:\Windows\Temp\ C:\Dokumente und Einstellungen\Administrator\Lokale Einstellungen\Temp\

C:\Dokumente und Einstellungen\Default User\Lokale Einstellungen\Temp\
C:\Dokumente und Einstellungen\DeinBenutzername\Lokale Einstellungen\Temp\

Windows Vista/ Windows7:

C:\Windows\Temp\
C:\Benutzer\DeinBenutzername\AppData\Local\Temp\
C:\Benutzer\Default\AppData\Local\Temp\

Erfahrungsgemäß sammelt sich in den etwas versteckten Ordnern nur sehr wenig an, insofern sind die CCleaner Voreinstellungen normalerweise ausreichend. Wer es trotzdem ausprobieren möchte, kann die entsprechenden Temp-Ordner als benutzerdefinierte Ordner im CCleaner eintragen.

Bleiben noch zwei Einstellungs-Rubriken übrig, einmal die Option Auschließen, wo du Ordner ausschließen kannst, die nicht in die Bereinigung einfließen sollen. Unter Erweitert sind noch ein paar grundsätzliche Einstellungen möglich, die du aber nicht verändern musst.

Registry-Cleaner:

Wie versprochen greifen wir an dieser Stelle das leidige Thema Registry-Cleaner noch einmal auf. Es ist wahrlich erschreckend, wie arglos einige Anwender diese Tools einsetzen, obwohl sie deren Wirkung weder verifizieren noch sicher einschätzen können. Besonders ärgerlich wird es, wenn einige Windows Foren sich zwar gegen die Verwendung dererlei Tools aussprechen, im Gegenzug aber Adsense Werbung mit eben diesen Tools ins Forum stellen, das ist wirklich "konsequent".

Um es auf den Punkt zu bringen, es existiert kein kausaler geschweige denn evidenzbasierter Beweis, das Registry Cleaner irgend etwas positives bewirken. Wenn ein solches Tool nach der Neuinstallation von Windows bei einer Analyse 700 zu optimierende Einträge findet, in der Masse sind das dann hauptsächlich Verweise auf nicht mehr vorhandene Dateien > nicht mehr vorhandene Verknüpfungen und nicht mehr vorhandene Programme, sollten wirklich alle Alarmglocken klingeln, weil das entbehrt nun wirklich jeglicher Logik.

In diesem Zusammenahng von "Tuning" zu sprechen ist ohnehin der blanke Hohn, aber es hält sich seit Jahren der Mythos, die Registry muss regelmäßig mit Hilfsprogrammen entschlackt werden, damit Windows optimal arbeitet. Dies ist de facto falsch, die Registry ist eine Datenbank, in der Windows und viele Programme entsprechende Konfigurationsdaten speichern.

Dort werden auch keinerlei ini-Dateien abgearbeitet sondern Datenbanken abgefragt, d.h. installierte Programme und Applikationen fragen ihre Keys und Einstellungen diesbezüglich bei Bedarf in den entsprechenden Hives ab. Das bedeutet im Klartext, dass nach einer Deinstallation des jeweiligen Programms diese Datenbankinformationen eben nicht mehr abgefragt werden, ergo haben sie auch keinen Einfluss mehr aufs System, ob sie nun da sind oder nicht.

Ebenso falsch ist die Behauptung, das die komplette Registry Datenbank permanent in den Arbeitsspeicher geladen wird und somit wertvollen Speicherplatz belegt und Windows so verlangsamt. Es wird definitiv nur das in den Speicher geladen, was verwendet wird: also die benötigten Hives, alles andere bleibt draußen, demzufolge kann die Registry niemals

Windows verlangsamen. Ganz davon abgesehn, dass ein einziger übereifriger Löschvorgang in der Registry ausreicht, um eurer Betriebssstem entscheidend zu kompromittieren.

Wenn dein Windows zu langsam ist, rüste deine Hardware auf, die Registry ist diesbezüglich der komplett falsche Ansprechpartner...

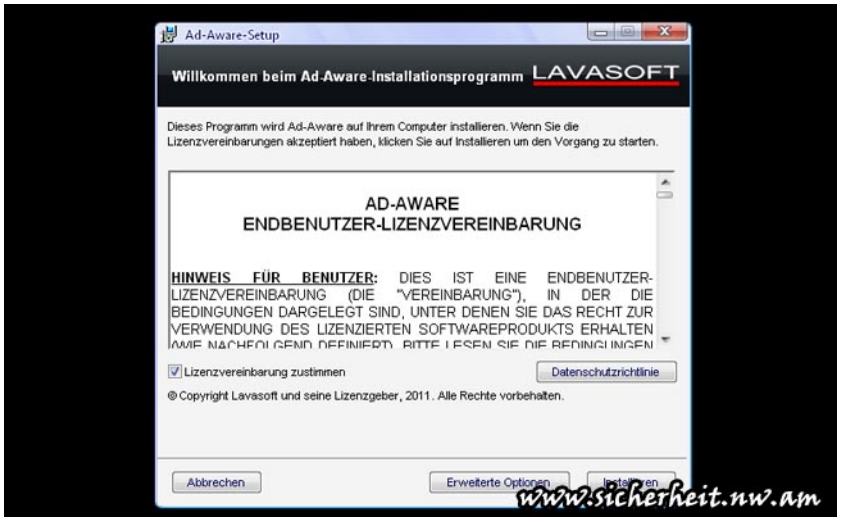
Ad-Aware

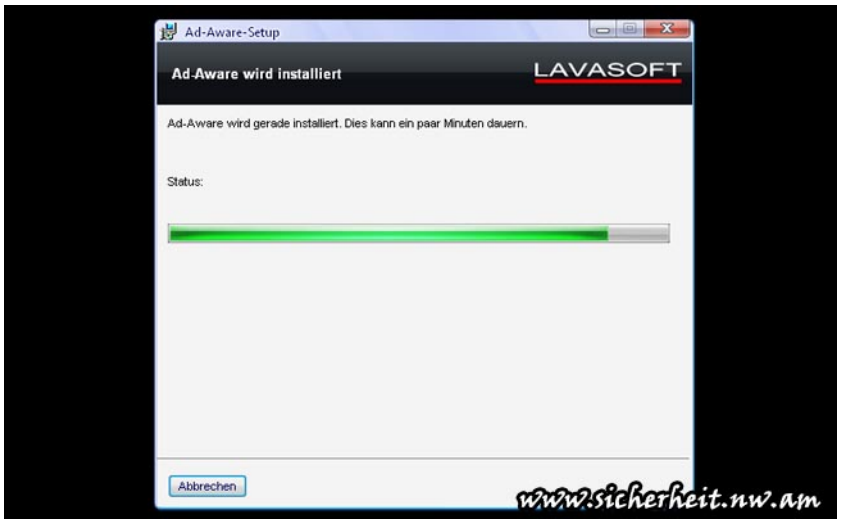
Zuerst lädst du dir die neuste Version von Ad-Aware herunter.

(Hier gezeigte Programmversion: **9.0.7)**

Ein Doppelklick auf die Installationsdatei und das Setup startet, hier wählen wir direkt die Sprache DEUTSCH.

Du akzeptierst die Lizenzvereinbarung und drückst auf ***Installieren***. Die Installation startet.


Ad-Aware-Setup
Willkommen beim Ad-Aware-Installationsprogramm
LAVASOFT
Dieses Programm wird Ad-Aware auf Ihrem Computer installieren. Wenn Sie die Lizenzvereinbarungen akzeptiert haben, klicken Sie auf Installieren um den Vorgang zu starten.
AD-AWARE
ENDBENUTZER-LIZENZVEREINBARUNG
HINWEIS FÜR BENUTZER: DIES IST EINE ENDBENUTZER-LIZENZVEREINBARUNG (DIE "VEREINBARUNG"), IN DER DIE BEDINGUNGEN DARGELEGT SIND, UNTER DENEN SIE DAS RECHT ZUR VERWENDUNG DES LIZENZIERTEN SOFTWAREPRODUKTS ERHALTEN
Lizenzvereinbarung zustimmen
Datenschutzrichtlinie
© Copyright Lavasoft und seine Lizenzgeber, 2011. Alle Rechte vorbehalten.
Abbrechen
Erweiterte Optionen
www.sicherheit.nw.am



Ist die Installation beendet entfernst du das Häckchen um imformiert zu werden und musst somit keine E-Post Adresse angeben. ***Fertig stellen.***

Ad-Aware-Setup
Installation ist abgeschlossen
LAVASOFT
Herzlichen Glückwunsch! Ad-Aware ist jetzt auf Ihrem Computer installiert.
Der Update-Manager wird gestartet, um die neuste Software und Definitionen von den Lavasoft-Servern herunter zu laden.
Ad-Aware starten
Bleiben Sie bestens informiert!
Um die Sicherheitsneuigkeiten und Sonderangebote von Lavasoft zu erhalten, geben Sie Ihren Namen und E-mail-Adresse unten ein:
Vorname:
Nachname:
E-mail:
Datenschutzrichtlinie
www.sicherheit.nw.am

Nun öffnet sich der ***Update Manager***und läd die neuste Software herunter.

Wenn das Programm gestartet ist, drückst du auf ***Jetzt scannen*** > ***Vollständiger Scan*** und anschließend auf ***Scannen*** um das System komplett zu durchsuchen.

Warum Festplatten verschlüsseln?

Es ist passiert, der bewaffnete Raubüberfall durch eine organisierte Bande der BRD GmbH hat stattgefunden. Dein wichtigstes Arbeitsgerät, ob privat oder geschäftlich, dein Rechner, wurde dir entführt. Schnüffleraugen warten begierig darauf, sich durch deine privatesten Vorgänge zu wühlen. Der Staatsanwalt hofft auf Beweise, die ihm einen großen Prozessauftritt ermöglichen und zu seiner Beförderung beitragen, der unbekannte Perverse vom Auswertedienst der Polizei hofft auf eine Pornosammlung, von der er eine private Sicherheitskopie erstellen möchte. Und du? Worauf hoffst du?

Du hast auf deinem Rechner ein Boot-Passwort, eine Sicherung auf BIOS-Ebene. Dieses verhindert Zugriffe von Unbefugten, beispielsweise jene des netten Zöllners auf dem Flughafen, der mal eben mit deinem Rechner in ein Nebenzimmer verschwindet. Angeblich möchte er dort herausfinden, ob der Rechner Sprengstoff enthält, tatsächlich will er dir einen Trojaner aufspielen. Man kann den Schergen eines parteidemokratischen Regimes in der Zerfallsphase wirklich nicht trauen.

Dann hast du als nächste Hürde ein Windows-Passwort. Dies ist eine sehr gute Maßnahme, die in Familien verhindert, dass sich der Papa den weitaus schnelleren Rechner des Sohnes schnappt, um unbeaufsichtigt ein paar wilde Schießereien in Echtzeit zu erleben. Umgekehrt nützt es wenig, denn kein Sohn wird den langweiligen Arbeitsrechner seines Vaters anwerfen wollen. Und wenn er muss? Nun, er kennt das Passwort natürlich, denn er hat es für Papi eingerichtet.

Die Polizei stört beides nicht, sie besitzt ein Tool, um diesen Schutz zu umgehen. Tool hieß früher einmal Werkzeug, in der Computersprache werden damit auch kleine nützliche Programme bezeichnet. Da die Polizei ein wenig altmodisch denkt, ist ihr Tool tatsächlich ein richtiges Werkzeug, ein Schraubendreher. Damit öffnen die Herren Ermittler - da es um Technik geht, brauchen Sie keine Frauen zu erwarten - das Gehäuse des Rechners und bauen die Festplatte aus.

Diese Festplatte schließen sie an einem Polizeirechner an, damit sind BIOS- und Windows-Passwort umgangen. Und schon strömen die Erkenntnisse auf den unverschämt feixenden Ermittler ein. Wobei ihm dieses Feixen jedoch schnell vergeht, wenn die einzige Erkenntnis, die er gewinnt, darin besteht, dass die Festplatte leider verschlüsselt ist, beispielsweise mit TrueCrypt. Jetzt kann er die bereitgelegten DVD-Rohlinge zur Übernahme der erhofften Porno-Sammlung wieder einpacken.

TrueCrypt gegen Polizei / FBI

Disks eines brasilianischen Bankiers waren unter anderem mit Truecrypt gesichert - Nach einem Jahr Knackversuche aufgegeben.

Immer wieder wird die Frage aufgeworfen, wie sicher eigentlich gebräuchliche Festplattenverschlüsselungstools tatsächlich sind, haben doch gerade staatliche Stellen in einigen Ländern massive Rechnerkapazitäten zur Hand. Die simple Weisheit, dass die

Sicherheit der eigenen Daten dabei vor allem von der Qualität des eigenen Passworts - und der Sorgfalt mit der man dieses geheim hält - abhängt, scheint sich nun in einem aktuellen Fall zu bestätigen.

Laut einem aktuellen Bericht ist es der US-Bundesbehörde FBI nicht gelungen, die Festplatten des brasilianischen Bankiers Daniel Dantas zu entschlüsseln. Ein Jahr lang hatte man versucht, die entsprechenden Passwörter ausfindig zu machen - dies ohne jeglichen Erfolg. Dabei griff man offenbar auf eine konventionelle Wörterbuchattacke zurück, bei der in schneller Reihenfolge immer wieder neue Passwortkombinationen ausprobiert werden. Vor dem FBI hatten es bereits die brasilianischen Behörden fünf Monate lang vergeblich auf dem selben Angriffsweg versucht.

Die bei einer Hausdurchsuchung im Juli 2008 beschlagnahmten Harddisks sind mittlerweile wieder nach Brasilien zurückgeschickt worden, womit die lokale Strafverfolgung in dieser Causa wohl an einem toten Punkt angekommen sein dürfte.

Nach der brasilianischen Rechtslage ist die Herausgabe der eigenen Passwörter gegenüber den Behörden nicht verpflichtend.

Auch in der BRD bist du nicht verpflichtet ein den Behörten ein Passwort zu geben.

In der BRD sieht die Rechtslage so aus: Das Schweigerecht gilt auch für private Passwörter! Die Polizei kann dich nicht in Haft stecken, wenn du das Passwort für deinen Computer nicht rausrückst! (Auch wenn es die Strafverfolgungsbehörden gerne anders hätten) Getreu nach dem Motto: "*Ach Sie haben wohl was zu verbergen...??*" Doch auch hier greift die Strafprozessordnung (StPO) zugunsten des Beschuldigten. Die Polizei kann nicht einfach "vermuten", dass auf deinem Computer strafrechtlich relevante Daten sind. Und in der Prazis zeigt sich, dass die Polizei Passwörter mit mehr als 12 Stellen gar nicht mehr versucht zu knacken..... Schon ist TrueCrypt installiert und gibt und gibt uns die Meldung ***Press enter to exit***. Also beenden wir die Installation durch betätigen der Eingabe-Taste.

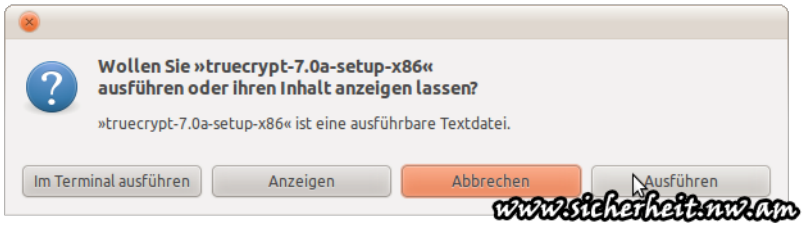
Fertig ist das Ganze und nun können wir auch unter Ubuntu mit TrueCrypt arbeiten.

Installation von TrueCrypt unter Ubuntu

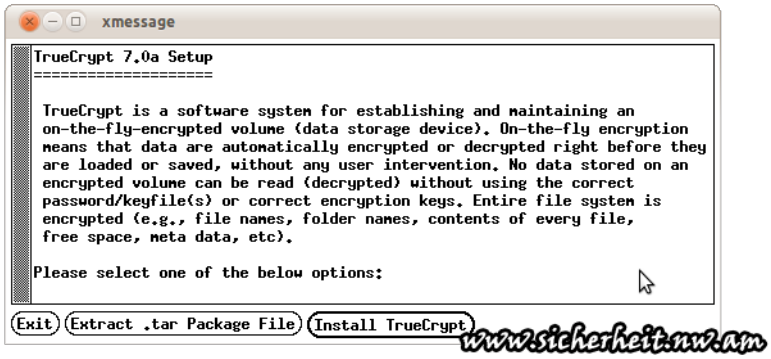
(Hier gezeigte Programmversion: **7.0a)**

Zuerst laden wir uns die neuste Version von TrueCrypt für Linux herunter.

Nachdem wir das erfolgreich getan haben, klicken wir mit der rechten Maustaste auf das Packet, klicken dann ***Hier entpacken***.



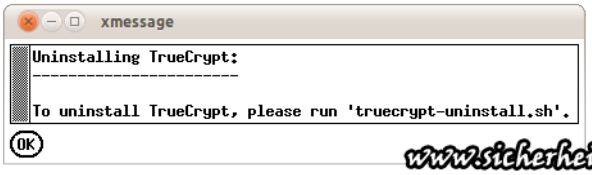
Nun können wir durch einen Doppelklick auf die entpackte Datei mit der Installation beginnen und bekommen anschließend ein Fenster angezeigt in dem wir auf ***Im Terminal Ausführen*** klicken.


xmessage
TrueCrypt 7.0a Setup
TrueCrypt is a software system for establishing and maintaining an on-the-fly-encrypted volume (data storage device). On-the-fly encryption means that data are automatically encrypted or decrypted right before they are loaded or saved, without any user intervention. No data stored on an encrypted volume can be read (decrypted) without using the correct password/keyfile(s) or correct encryption keys. Entire file system is encrypted (e.g., file names, folder names, contents of every file, free space, meta data, etc).
Please select one of the below options:
Exit
Extract .tar Package File
Install TrueCrypt
www.sicherheit.nw.am

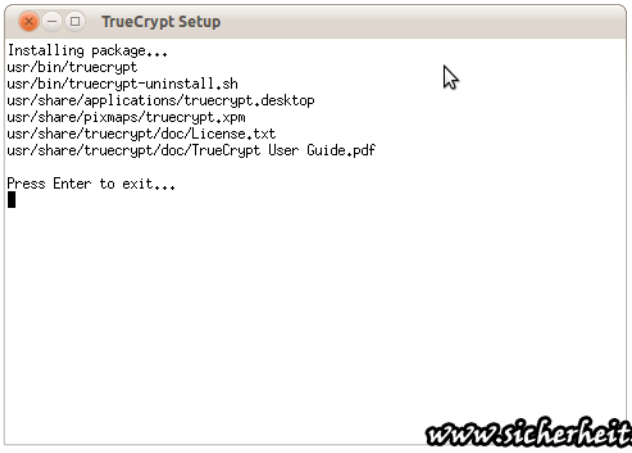
Jetzt klicken wir auf ***Install TrueCrypt***.

xmessage
Before you can use, extract, or install TrueCrypt, you must accept these license terms.
IMPORTANT: By clicking the left button below this text field, you accept these license terms and agree to be bound by and to comply with them. Press Page Down key or use the scroll bar to see the rest of the license.
TrueCrypt License Version 3.0
Software distributed under this license is distributed on an "AS IS" BASIS WITHOUT WARRANTIES OF ANY KIND. THE AUTHORS AND DISTRIBUTORS OF THE SOFTWARE DISCLAIM ANY LIABILITY. ANYONE WHO USES, COPIES, MODIFIES, OR (RE)DISTRIBUTES ANY PART OF THE SOFTWARE IS, BY SUCH ACTION(S), ACCEPTING AND AGREEING TO BE BOUND BY ALL TERMS AND CONDITIONS OF THIS LICENSE. IF YOU DO NOT ACCEPT THEM, DO NOT USE, COPY, MODIFY, NOR (RE)DISTRIBUTE THE SOFTWARE, NOR ANY PART(S) THEREOF.
I. Definitions
1. "This Product" means the work (including, but not limited to, source code, graphics, texts, and accompanying files) made available under and governed by this version of this license ("License"), as may be indicated by, but is not limited to, copyright notice(s) attached to or included in the work.
2. "You" means (and "Your" refers to) an individual or a legal entity (e.g., a non-profit organization, commercial organization, government agency, etc.) exercising permissions granted by this License.
3. "Modification" means (and "modify" refers to) any alteration of This Product, including, but not limited to, addition to or deletion from the substance or structure of This Product, translation into another language, repackaging, alteration or removal of any file included with This Product, and addition of any new files to This Product.
I accept and agree to be bound by the license terms
I do not accept
www.sicherheit.nw.am

Aktzeptieren dann die Lizenzbestimmungen.



Klicken in der nächsten Meldung, nachdem wir den Hinweis zur Deinstallation von Truecrypt wahrgenommen haben haben, auf ***OK***.



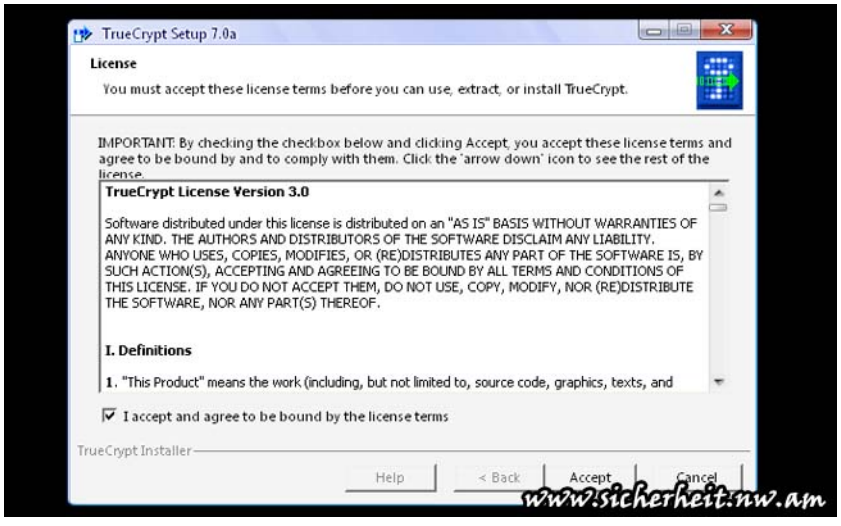
Schon ist TrueCrypt installiert und gibt und gibt uns die Meldung ***Press enter to exit***. Also beenden wir die Installation durch betätigen der Eingabe-Taste.

Fertig ist das Ganze und nun können wir auch unter Ubuntu mit TrueCrypt arbeiten.

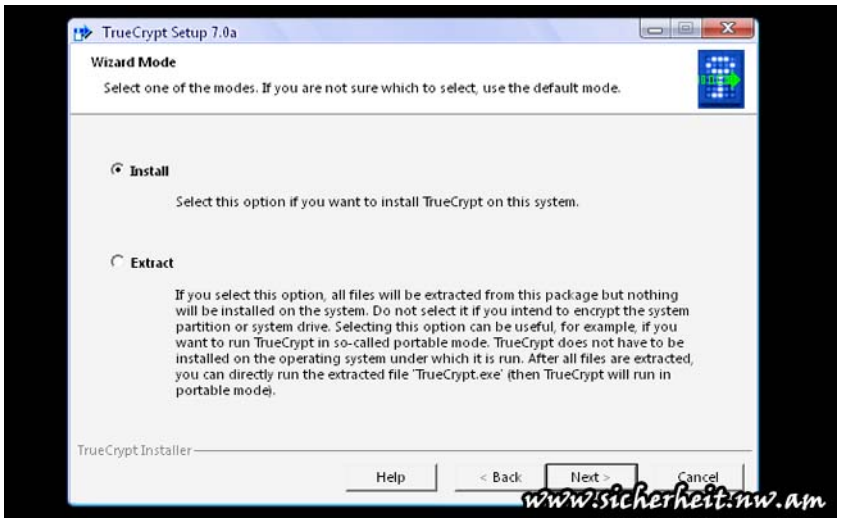
Installation von TrueCrypt unter Windows

Zuerst laden wir uns die neuste Version von **TrueCrypt** herunter.

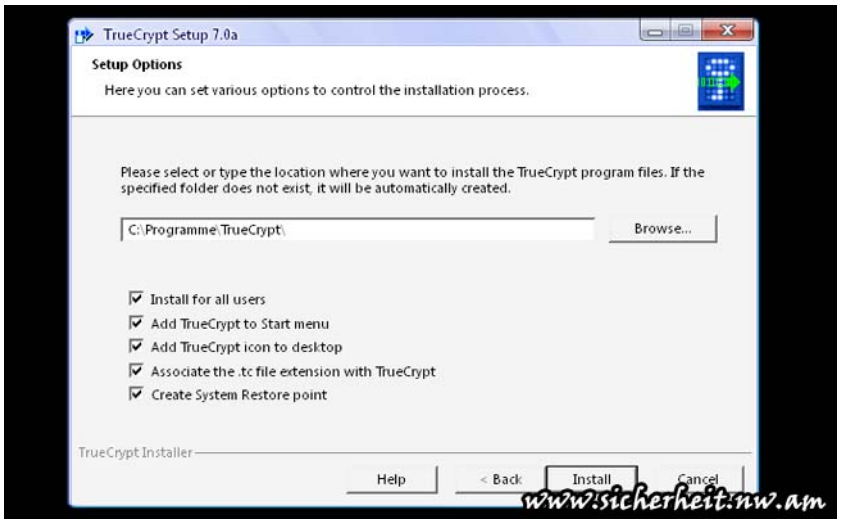
Nachdem wir die Datei mit einem Doppelklick geöffnet haben akzeptieren wir die Lizenzvereinbarung und drücken auf ***Accept*** und direkt auf ***Next***.


TrueCrypt Setup 7.0a
License
You must accept these license terms before you can use, extract, or install TrueCrypt.
IMPORTANT: By checking the checkbox below and clicking Accept, you accept these license terms and agree to be bound by and to comply with them. Click the 'arrow down' icon to see the rest of the license.
TrueCrypt License Version 3.0
Software distributed under this license is distributed on an "AS IS" BASIS WITHOUT WARRANTIES OF ANY KIND. THE AUTHORS AND DISTRIBUTORS OF THE SOFTWARE DISCLAIM ANY LIABILITY.
ANYONE WHO USES, COPIES, MODIFIES, OR (RE)DISTRIBUTES ANY PART OF THE SOFTWARE IS, BY SUCH ACTION(S), ACCEPTING AND AGREEING TO BE BOUND BY ALL TERMS AND CONDITIONS OF THIS LICENSE. IF YOU DO NOT ACCEPT THEM, DO NOT USE, COPY, MODIFY, NOR (RE)DISTRIBUTE THE SOFTWARE, NOR ANY PART(S) THEREOF.
I. Definitions
1. "This Product" means the work (including, but not limited to, source code, graphics, texts, and
I accept and agree to be bound by the license terms
TrueCrypt Installer
Help
< Back
Accept
Cancel
www.sicherheit.nw.am

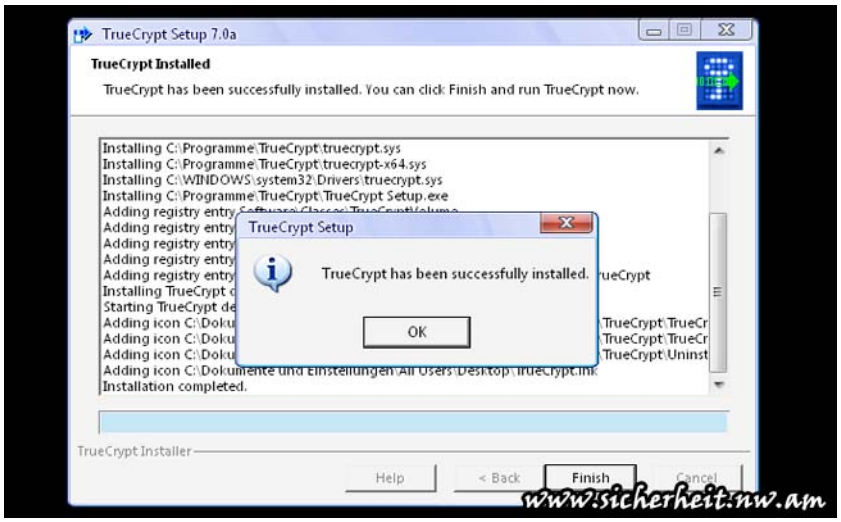
Natürlich wollen wir das Programm auf dem Computer installieren und nicht nur entpacken. Wir wählen also **Install**


TrueCrypt Setup 7.0a
Wizard Mode
Select one of the modes. If you are not sure which to select, use the default mode.
Install
Select this option if you want to install TrueCrypt on this system.
Extract
If you select this option, all files will be extracted from this package but nothing will be installed on the system. Do not select it if you intend to encrypt the system partition or system drive. Selecting this option can be useful, for example, if you want to run TrueCrypt in so-called portable mode. TrueCrypt does not have to be installed on the operating system under which it is run. After all files are extracted, you can directly run the extracted file 'TrueCrypt.exe' (then TrueCrypt will run in portable mode).
TrueCrypt Installer
Help
< Back
Next >
Cancel
www.sicherheit.nw.am

In folgendem Fenster wird nun der Installationsort festgelegt sowie ein Wiederherstellungspunkt für Windows angelegt.


TrueCrypt Setup 7.0a
Setup Options
Here you can set various options to control the installation process.
Please select or type the location where you want to install the TrueCrypt program files. If the specified folder does not exist, it will be automatically created.
C:\Programme\TrueCrypt\
Browse...
Install for all users
Add TrueCrypt to Start menu
Add TrueCrypt icon to desktop
Associate the .tc file extension with TrueCrypt
Create System Restore point
TrueCrypt Installer
Help
< Back
Install
Cancel
www.sicherheit.nw.am

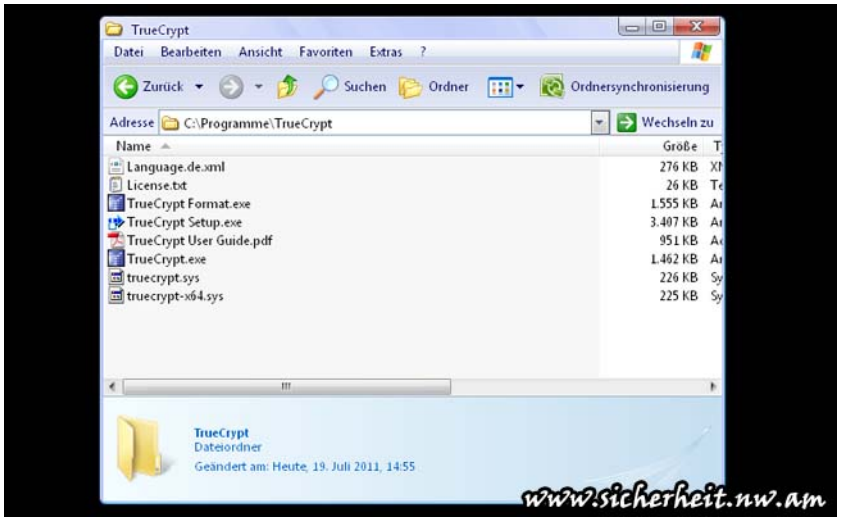
Wir bestätigen nun mit ***Install*** und die Installation beginnt.



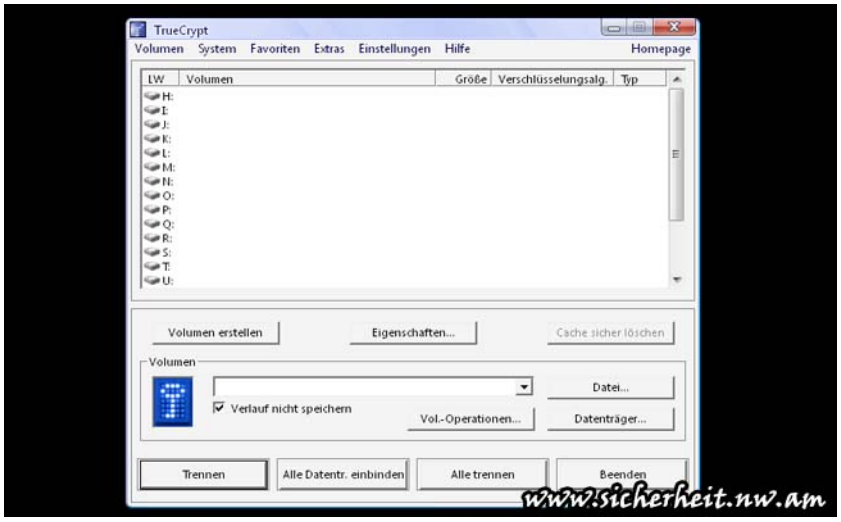
Ist die Installation abgeschlossen bestätigen wir mit ***OK*** und ***Finish***.

Nun laden wir uns HIER die Deutsche Sprachdatei herunter.

Haben wir die Datei nun auf unserem Computer öffnen wir sie und extrahieren/kopieren die Datei ***Language.de.xml*** in den Ordner ***C:/Programme/TrueCrypt***.



Nun können wir das Programm über das Startmenü oder die Desktop-Verknüpfung starten. Es erscheint direkt die Frage ob wir das Benutzerhandbuch lesen möchten. Falls man der englischen Sprache mächtig ist und viel Zeit hat, kann man dies tun. In unserem Falle überspringen wir diesen Punkt. Wir haben nun das Hauptfenster vor Augen.

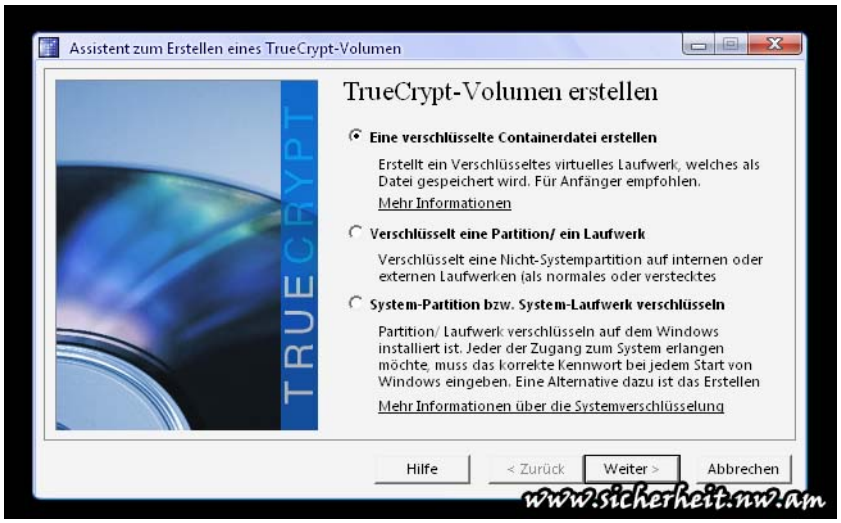


Erstellen von Datentresoren

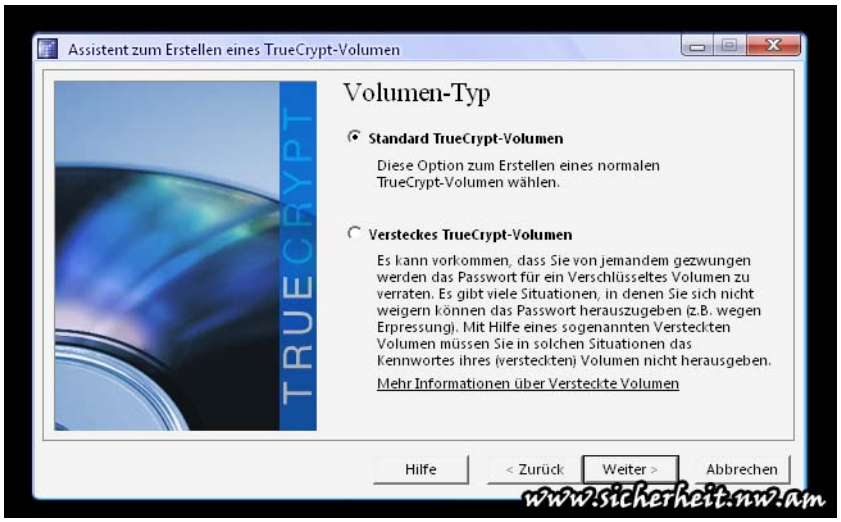
Die einfachste Möglichkeit seine privaten Daten zu verschlüsseln, ist die mittels eines Datentresors. Diese sogenannte Containerdatei wird beim Erstellen mit Zufallsdaten gefüllt und kann anhand des Passwortes in das System eingehängt werden. Dieser Tresor erscheint dann im Arbeitsplatz als neues Laufwerk. Man kann ihn auch wie ein solches behandeln. Daten davon lesen, löschen, ihn mit neuen beschreiben – alles geschieht verschlüsselt in Echtzeit. Diese Tresore kann man entweder auf seiner Festplatte oder auf mobilen Datenträgern erstellen. Wunderbar eignet sich dafür natürlich die Verschlüsselung von USB-Speicherstiften.

Im Hauptfenster drücken wir auf ***Volumen erstellen***.

Hier wählen wir ***Eine Containerdatei erstellen*** und drücken auf ***Weiter***.


Assistent zum Erstellen eines TrueCrypt-Volumen
TrueCrypt-Volumen erstellen
Eine verschlüsselte Containerdatei erstellen
Erstellt ein Verschlüsseltes virtuelles Laufwerk, welches als Datei gespeichert wird. Für Anfänger empfohlen.
Mehr Informationen
Verschlüsselt eine Partition/ ein Laufwerk
Verschlüsselt eine Nicht-Systempartition auf internen oder externen Laufwerken (als normales oder verstecktes
System-Partition bzw. System-Laufwerk verschlüsseln
Partition/ Laufwerk verschlüsseln auf dem Windows installiert ist. Jeder der Zugang zum System erlangen möchte, muss das korrekte Kennwort bei jedem Start von Windows eingeben. Eine Alternative dazu ist das Erstellen
Mehr Informationen über die Systemverschlüsselung
Hilfe
< Zurück
Weiter >
Abbrechen
TRUECRYPT
www.sicherheit.nw.am

Nun wählen wir ***Standart TrueCrypt-Volume*** und ***Weiter***.


Assistent zum Erstellen eines TrueCrypt-Volumen
Volumen-Typ
Standard TrueCrypt-Volumen
Diese Option zum Erstellen eines normalen TrueCrypt-Volumen wählen.
Verstecktes TrueCrypt-Volumen
Es kann vorkommen, dass Sie von jemandem gezwungen werden das Passwort für ein Verschlüsseltes Volumen zu verraten. Es gibt viele Situationen, in denen Sie sich nicht weigern können das Passwort herauszugeben (z.B. wegen Erpressung). Mit Hilfe eines sogenannten Versteckten Volumen müssen Sie in solchen Situationen das Kennwortes ihres (versteckten) Volumen nicht herausgeben.
Mehr Informationen über Versteckte Volumen
Hilfe
< Zurück
Weiter >
Abbrechen
TRUECRYPT
www.sicherheit.nw.am

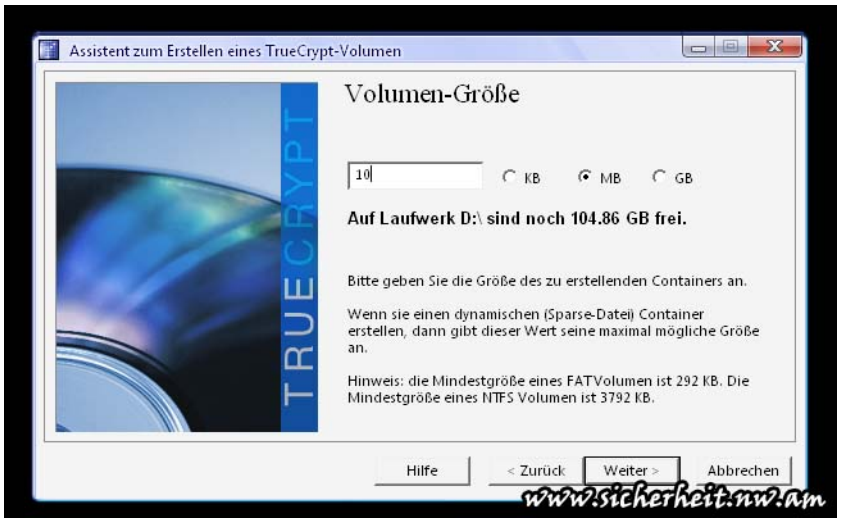
Im folgenden Fenster müssen wir nun den Speicherort sowie den Dateinamen des Tresors bestimmen. Ersteinmal müssen wir auf dem Computer, wo auch immer wir den Container haben möchten, per Rechtsklick auf der Computer-Maus eine Datei erstellen. Der Name sowie die Dateiendung spielen hierbei überhaupt keine Rolle! Wir haben

unsere Datei nun "*tresor*" mit der Endung "*.tc*" gatauft und in in das Verzeichnis des Laufwerk "D:\" gelegt. ***Weiter***!

Assistent zum Erstellen eines TrueCrypt-Volumen
Volumen-Speicherort
D:\tresor.tc
Datei...
Verlauf nicht speichern
Ein TrueCrypt Volumen kann in einer Datei liegen (eine TrueCrypt Containerdatei), welche sich auf einer Festplatte, einer Partition, einem USB-Stick usw. befinden kann. Eine TrueCrypt Containerdatei verhält sich genau wie eine normale Datei (sie kann zum Beispiel wie eine normale Datei kopiert, bewegt oder gelöscht werden). Klicken Sie auf "Datei..." um einen Dateinamen und den Speicherort für die Containerdatei zu wählen.
ACHTUNG: Wenn Sie eine bestehende Datei wählen wird TrueCrypt diese NICHT verschlüsseln; die Datei wird gelöscht und mit der Containerdatei ersetzt. Sie können bestehende Dateien verschlüsseln indem Sie diese später in den neuen
Hilfe
< Zurück
Weiter >
Abbrechen
TRUECRYPT
www.sicherheit.nw.am

Als nächstes wird der Algorithmus ausgewählt, welcher die Grundlage der Verschlüsselung bieten soll. Wir wählen am Besten den ***Advanced Encryption Standard (AES)*** oder ***Twofish***. Diese bieten eine Sichere Verschlüsselung bei wenig Systembelastung. Als Hash-Algorithmus können wir *RIPEMD-160* lassen.
Weiter!

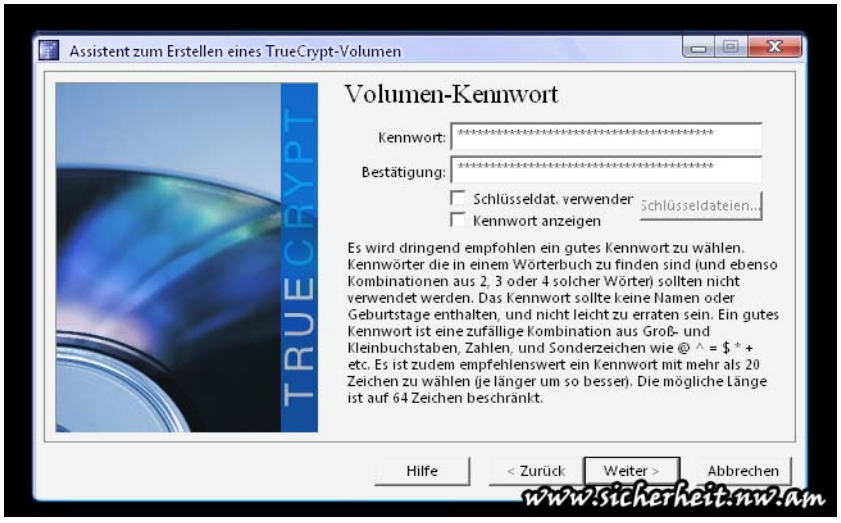
Nun wählen wir die *Größe* des Tresors, welche er am Ende haben soll. Diese richtet sich natürlich danach, was ihr alles darin speichern wollt. Wenn es lediglich für ein paar Dokumente sein soll, reichen wenige Megabyte. Sollen jedoch ganze USB-Speicherstifte verschlüsselt werden, richtet sich die Größe nach der Stiftgröße. Ist er *1 Gigabyte* groß empfiehlt es sich für rund *800 Megabyte* zu wählen. Die restlichen 200 Megabyte dienen dem Programm TrueCrypt falls es ein Rechner, auf dem man den Tresor öffnen will, noch nicht installiert hat und andere Dateien, die nicht zwingendermaßen verschlüsselt werden müssen oder zum schnellen Dateiaustausch mit Freunden und Kollegen dienen.
Weiter!


Assistent zum Erstellen eines TrueCrypt-Volumen
Volumen-Größe
10
KB
MB
GB
Auf Laufwerk D:\ sind noch 104.86 GB frei.
Bitte geben Sie die Größe des zu erstellenden Containers an.
Wenn sie einen dynamischen (Sparse-Datei) Container erstellen, dann gibt dieser Wert seine maximal mögliche Größe an.
Hinweis: die Mindestgröße eines FATVolumen ist 292 KB. Die Mindestgröße eines NTFS Volumen ist 3792 KB.
Hilfe
< Zurück
Weiter >
Abbrechen
TRUECRYPT
www.sicherheit.nu.am

Nun müssen wir ein Passwort wählen.

Bitte Abschnitt Passwortwahl weiter unten beachten!

Weiter!

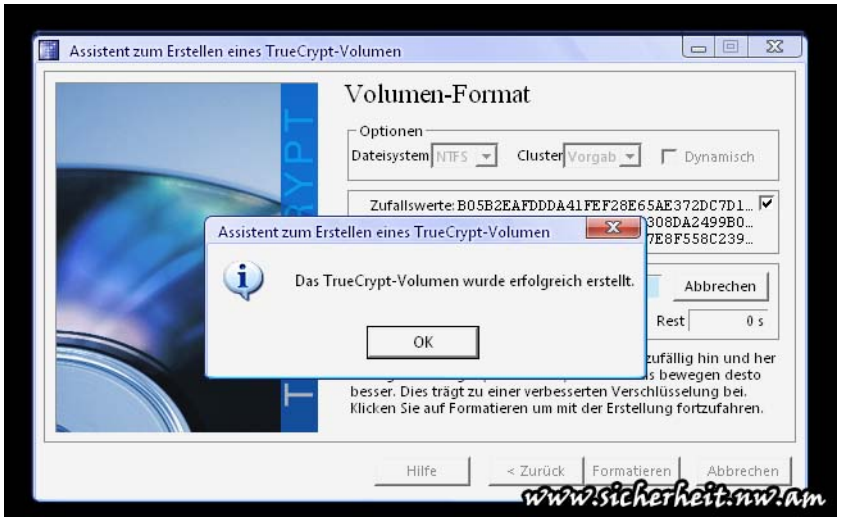

Assistent zum Erstellen eines TrueCrypt-Volumen
Volumen-Kennwort
Kennwort:
Bestätigung:
Schlüsseldat. verwenden
Schlüsseldateien...
Kennwort anzeigen
Es wird dringend empfohlen ein gutes Kennwort zu wählen. Kennwörter die in einem Wörterbuch zu finden sind (und ebenso Kombinationen aus 2, 3 oder 4 solcher Wörter) sollten nicht verwendet werden. Das Kennwort sollte keine Namen oder Geburtstage enthalten, und nicht leicht zu erraten sein. Ein gutes Kennwort ist eine zufällige Kombination aus Groß- und Kleinbuchstaben, Zahlen, und Sonderzeichen wie @ ^ = $ * + etc. Es ist zudem empfehlenswert ein Kennwort mit mehr als 20 Zeichen zu wählen (je länger um so besser). Die mögliche Länge ist auf 64 Zeichen beschränkt.
Hilfe
< Zurück
Weiter >
Abbrechen
TRUECRYPT
www.sicherheit.nu.am

Im folgenden Fenster wählen wir das Dateisystem. Mit ***NTFS*** machen wir nichts falsch und weiter geht's mit ***Formatieren***.

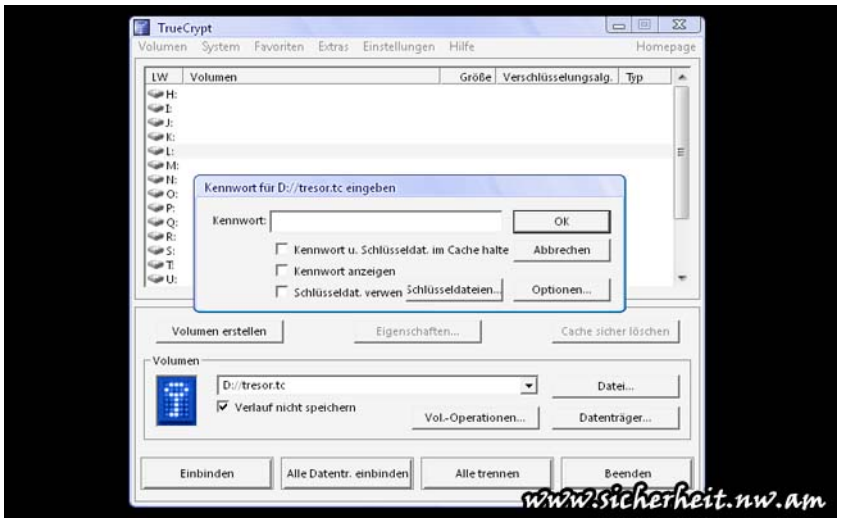
WICHTIG, Text beachten:

Den Mauszeiger in diesem Fenster zufällig hin und her bewegen.
Je länger (min. 30 Sekunden) du die Maus bewegst, desto besser.
Dies trägt zu einer verbesserten Verschlüsselung bei.

Wenn die Verschlüsselung fertig ist bestätigen wir die Meldung mit ***OK***. Jetzt wird noch einmal ***Weiter*** gedrückt und wir sind wieder am Anfang. Falls wir keinen weiteren Tresor erstellen möchten, drücken wir auf ***Abbrechen***.



Möchten wir diesen Tresor nun in unser System einbinden, wählen wir ihn im Hauptfenster unter ***Datei*** aus, wählen oben einen ***Laufwerksbuchstaben*** und drücken auf ***Einbinden***. Wir geben das Passwort ein und bestätigen mit ***OK***.



Je nachdem welchen Laufwerksbuchstaben du gewählt hast, erscheint nun im Arbeitsplatz das neue Laufwerk, welches solange der Tresor ins System eingebunden ist, wie ein handelsüblicher USB-Speicherstift benutzt werden kann. Möchten wir den Tresor schließen drücken wir auf ***Trennen*** im Hauptfenster.

Passwortwahl

Passwortgeschützte Daten sind nur dann sicher, wenn auch das Passwort, mit denen sie verschlüsselt wurden, sicher ist.

Der sicherste Verschlüsselungsalgorithmus nützt wenig, wenn als Schlüssel ein einfach zu erratendes Passwort verwendet wird.

Dabei meint "einfach zu erraten" nicht nur Personen, die z.B. die Namen Ihrer (Ex-)Partnerin, Freundin, Haustiere, Kinder oder Lieblingsbands sowie Wörter zu Ihren Hobbies oder aus Ihren Interessens- und Arbeitsgebieten ausprobieren, um an Ihre Daten zu kommen.

Bei der heutigen Rechenleistung können selbst günstigste Standard-Computer sehr schnell sehr viele Passwörter und damit ganze Wörterbücher verschiedenster Sprachen sowie Namens- und Passwortlisten mit hunderttausenden von Einträgen sowie gängige Kombinationen und Passwortanhängsel innerhalb kürzester Zeit vollautomatisch durchprobieren.

So dürfen einzelne Wörter, Nummern, ein Datum oder Namen sowie gängige Sätze (z.B. Zitate oder Parolen) auch in Kombination oder mit evtl. angehängten Zahlen nicht als ausreichender Schutz betrachtet werden.

Die Frage, die sich einem stellen sollte, wenn man sich ein neues Passwort zulegen muss, sollte stets sein: Wie kann ich es lange genug machen und mir es trotzdem einfach merken können?

Ein sicheres Passwort erkennt man an den folgenden Aspekten:

- Es beinhaltet mindestens(!) 8 Zeichen

- Es beinhaltet große und kleine Buchstaben (a-z, A-Z)
- Es beinhaltet Zahlen (0-9)
- Es beinhaltet Sonderzeichen („_“, „+“, „?“, „#“, „&“, „%“)

Befolgt man nun diese 4 Regeln entstehen z.B. Passwörter wie „**j7%_P+1r&U**“, „**e56U_W?a0**“ und so weiter. Zugegebenermaßen sind solche wirren Zeichenfolgen für den Ungeübten ziemlich schlecht zu merken. Deshalb geben wir weiterführend den Rat:

Baut euch eure Passwörter aus Sätzen!

Dadurch sind sie nicht nur einfacher zu merken, sondern gewinnen ebenfalls erheblich an Größe. Folgend nun zwei Beispiele:

Nachbar Müllers Hund heißt Bodo -
„**0NACHbar1_2MuElLeRs?hund_8_hEiSsT_8_boDO**“

Susi hat lange blonde Haare - „**sUSi=123=HAT_lANGe%bl0nde&H44Re**“

Solche Passwörter sind sehr sicher und ebenso einfach zu merken, oder? Nach mehrmaligem Probetippen hat man sie sicher drauf. Du siehst außerdem, dass wir an der einen oder anderen Stelle Zahlen anstatt Buchstaben genutzt haben. Diese Schreibvariation (auch Leet-Speak genannt) bietet die Möglichkeit, ähnlich aussehende Zahlen und Zeichen einfach anstatt den ursprünglichen Buchstaben zu nutzen. Hier eine kleine Liste:

A	=	B	=	C	=	D	=	E	=	G	=	H	=	I	=	K	=	L	=	M
4		8		(		|)		3		9		|-|		1		|<		|_		|V|
=	N	=	O	=	R	=	S	=	X	=										
	||		0		2		5		><											

Neben diesen Vorschlägen kann man natürlich auch eigene Kreationen nutzen. Es ist alles Recht, sei es noch so komisch, es dient letztendlich eurer Sicherheit.

Es gibt wage Schätzungen wie lange ein Supercomputer für das Knacken eines solch langen Passwortes brauchen würde. Diese sind aber definitiv nicht aussagefähig, da die Technologie

voranschreitet und damit die Verarbeitungsgeschwindigkeit eines Rechenprozessors stets zunimmt.

Wir raten deshalb: **Besser ein Zeichen zu viel als zu wenig**!

Wenn sich der Staat auch überlegt für das Knacken DEINES Passwortes einen Supercomputer für 5-6-stellige Euro-Summen zu beauftragen, steht es nichtmehr in unserer Macht dies zu verhindern, haben wir aber alles Mögliche getan, unser Passwort so sicher wie möglich zu gestalten und es der Maschine so schwer wie nur möglich zu machen.

Eure persönlichen Passwörter sind die Schlüssel zu euren Informationen. Geht also sehr vorsichtig mit ihnen um und notiert sie euch nirgends, euren Haustürschlüssel würdet ihr in der Öffentlichkeit auch nicht überall hinlegen, oder? Ebenso wenig solltet ihr ungeschützte Passwortlisten auf dem Rechner erstellen oder diese im Mobiltelefon speichern. Falls ihr dennoch zu viele Passwörter besitzt um sie euch merken zu können, dann nutzt z.B. Programme wie KeePass um sie sicher zu verwalten.

Desweiteren legen wir dir folgenden Rat ans Herzen: Um die Sicherheit deines Passwortes stets zu gewährleisten, solltest du es regelmäßig, im Idealfall alle 6-9 Monate, ändern. Dies schützt dich davor, dass Dritte dein Passwort eventuell erfasst haben und es ohne deine Kenntnis ab und zu selbst nutzen.

Geheimhaltung des eigenen Passwortes:

Das sicherste Passwort ist nicht mehr sicher wenn man es jedem weitergibt dem man vertraut. Ein Passwort sollte man immer nur für sich behalten. Auch dem Lebens- oder Ehepartner sollte man ein Passwort niemals mitteilen. Man kann jetzt sagen, dass es ein Vertrauensbruch darstellt aber auch unbeabsichtigt kann dadurch das sicherste Passwort an die falschen Leute geraten. Zum Beispiel wenn das Passwort leichtsinnig auf der Arbeit unter Beobachtung eingegeben oder sogar aufgeschrieben wird. Gerade aber aufschreiben oder in eine Textdatei speichern sollte man ein Passwort nicht.

Dies ist nur eine Anregung zur Zusammenstellung eines Passworts. Der Fantasie sind dabei eigentlich keine Grenzen gesetzt. Das Gegenteil ist der Fall. Wenn man sich eine eigene Methode zur Erstellung eines Passwortes einfallen lässt ist es sogar noch individueller und damit auch sicherer.

Aufbewahrung von Passwörtern

Bei solch einfallsreichen und langen Passwörtern stellt sich uns ein weiteres Problem in die Quere:

Wenn man für jeden Anbieter, bei dem man ein Passwort benötigt, ein anderes, 20-Zeichen langes, Passwort mit Zahlen und Sonderzeichen nutzt, wie soll man sich diese dann bitteschön alle merken?

Der ein oder andere mag zwar ein Gedächtnisgenie sein und somit keine Probleme damit haben, der Großteil aber würde sich diese auf einem Stück Papier oder gar auf dem Rechner notieren. Um diesem erheblichen Sicherheitsrisiko entgegenzuwirken, gibt es ein Programm namens *KeePass Password Safe*.

Dieses Programm legt eine, mit den Algorithmen AES und Twofish, vollverschlüsselte Datenbank an in der die verschiedenen Passwörter mit dem dazugehörigen Anbieter als Datensätze angelegt werden. Man muss sich somit nur noch das Haupt-Passwort für den Zugang zu dem Programm merken. Dieses sollte natürlich besonders sicher sein und mit viel Bedacht gewählt werden, ebenfalls regelmäßig gewechselt werden.

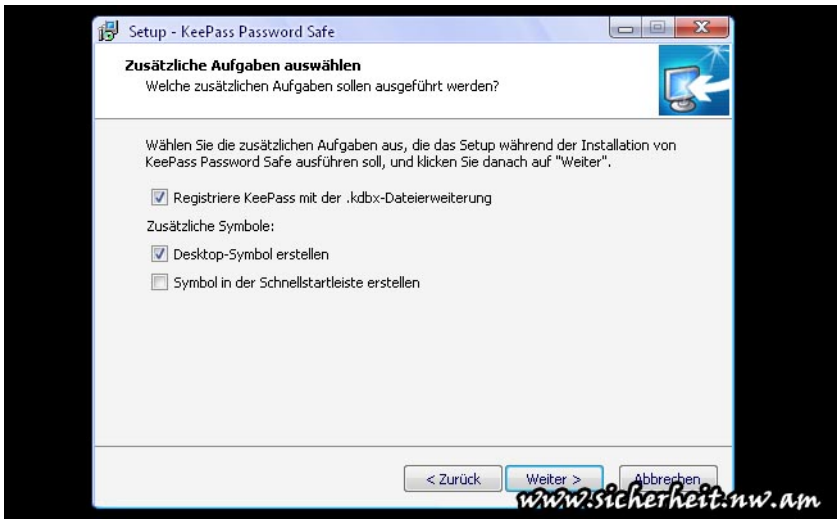
Hier gezeigte Programmversion: **2.16**

Zuerst laden wir die neuste Version von KeePass Password Safe sowie die deutsche Sprachdatei herunter.

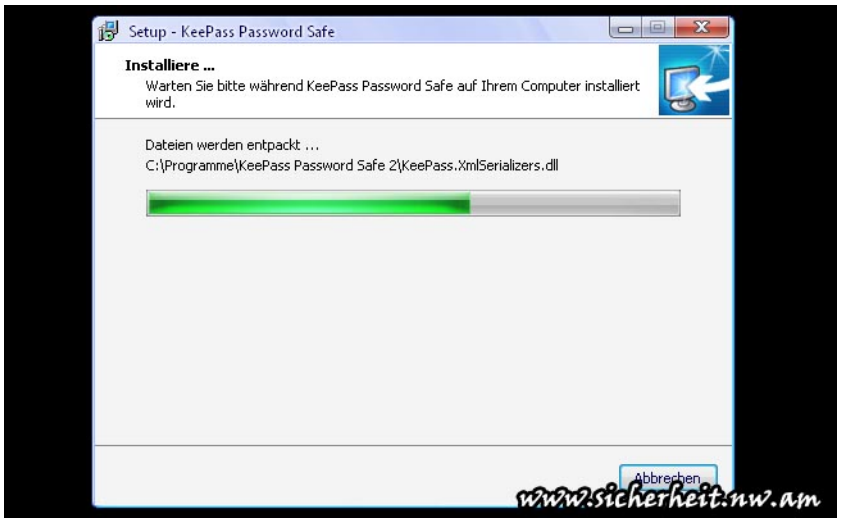
Wir öffnen nun die Installationsdatei, wählen die Sprache *Deutsch* und bestätigen.

Nachdem wir einmal ***Weiter*** gedrückt haben akzeptieren wir die Lizenzvereinbarung und drücken weitere 3 mal auf ***Weiter***.

Da wir das Programm leicht wiederfinden möchten machen wir ein Häckchen in das Feld ***Desktop-Symbol erstellen***. Weiter gehts mit ***Weiter***.


Setup - KeePass Password Safe
Zusätzliche Aufgaben auswählen
Welche zusätzlichen Aufgaben sollen ausgeführt werden?
Wählen Sie die zusätzlichen Aufgaben aus, die das Setup während der Installation von KeePass Password Safe ausführen soll, und klicken Sie danach auf "Weiter".
Registriere KeePass mit der .kdbx-Dateierweiterung
Zusätzliche Symbole:
Desktop-Symbol erstellen
Symbol in der Schnellstartleiste erstellen
< Zurück
Weiter >
Abbrechen
www.sicherheit.nw.am

Als nächstes wird auf ***Installieren*** gedrückt und das Programm kopiert sich auf die Festplatte.
Noch auf ***Fertig stellen*** gedrückt und die Installation ist abgeschlossen.

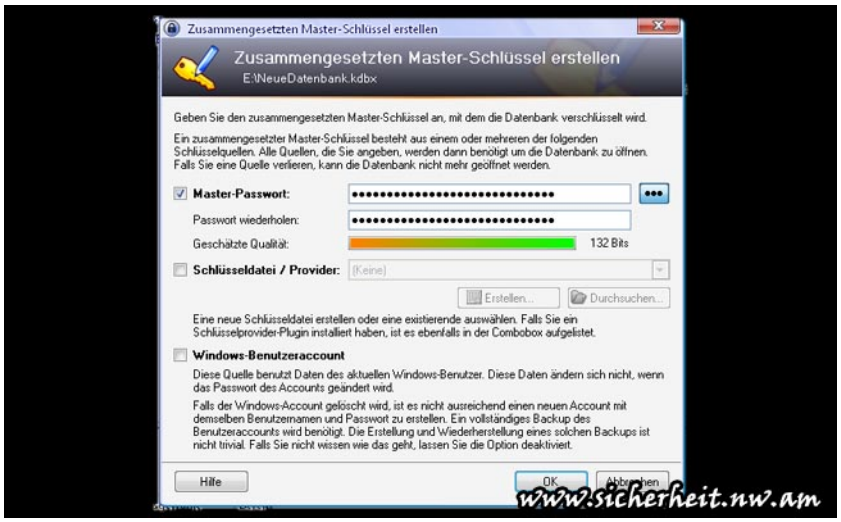

Setup - KeePass Password Safe
Installiere ...
Warten Sie bitte während KeePass Password Safe auf Ihrem Computer installiert wird.
Dateien werden entpackt ...
C:\Programme\KeePass Password Safe 2\KeePass.XmlSerializers.dll
Abbrechen
www.sicherheit.nw.am

Setup - KeePass Password Safe
Beenden des KeePass Password Safe Setup-Assistenten
Das Setup hat die Installation von KeePass Password Safe auf Ihrem Computer abgeschlossen. Die Anwendung kann über die installierten Programm-Verknüpfungen gestartet werden.
Klicken Sie auf "Fertigstellen", um das Setup zu beenden.
KeePass starten
Fertigstellen
www.sicherheit.nw.am

Nun öffnen wir die ebenfalls zuvor heruntergeladene Sprachdatei und kopieren die Datei ***German.lngx*** in das Verzeichnis in welches wir auch das Programm installiert haben, üblicherweise ***C:/Programme/KeePass Password Safe 2***.

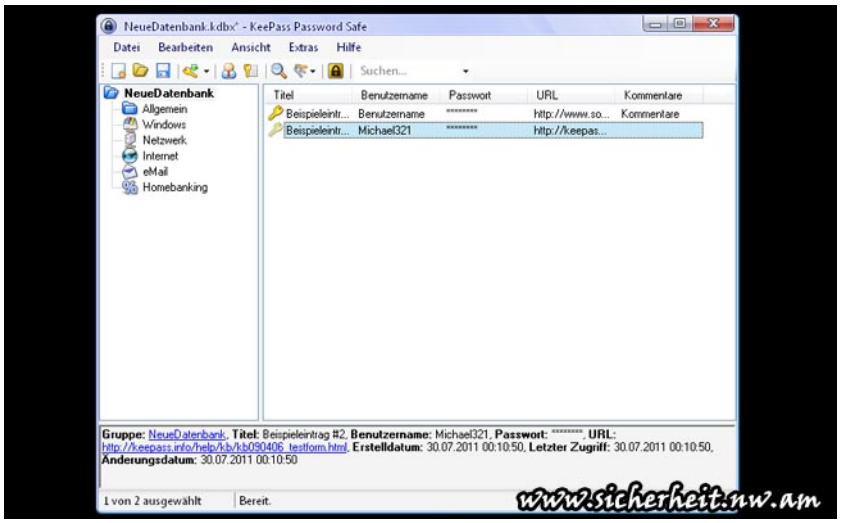
Nachdem wir das Programm gestartet haben, drücken wir oben auf ***View*** > ***Change Language***, dort wählen wir die Sprache ***Deutsch*** aus und bestätigen mit ***Ja***, das Programm startet nun selbstständig neu.

Im Hauptfenster wählen wir nun oben *Datei* > *Neu* und erstellen mit einem sicheren Passwort eine Datenbank.

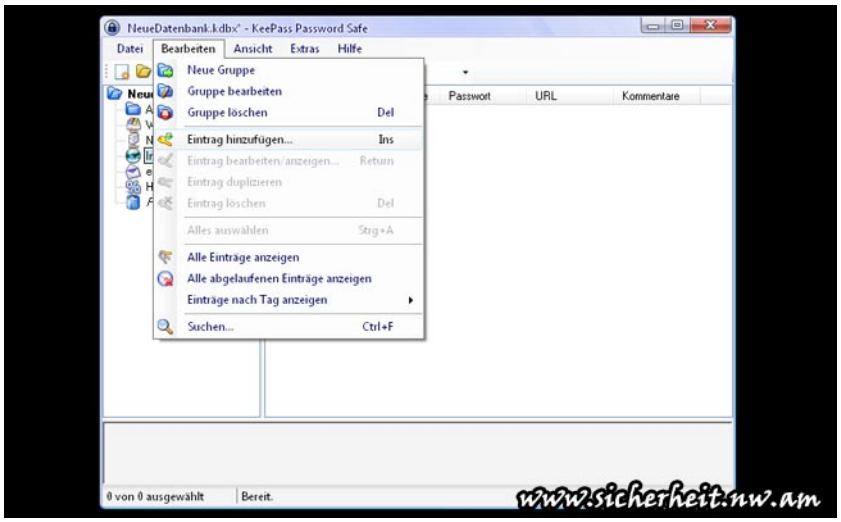

Zusammengesetzten Master-Schlüssel erstellen
Zusammengesetzten Master-Schlüssel erstellen
E:\NeueDatenbank.kdbx
Geben Sie den zusammengesetzten Master-Schlüssel an, mit dem die Datenbank verschlüsselt wird.
Ein zusammengesetzter Master-Schlüssel besteht aus einem oder mehreren der folgenden Schlüsselquellen. Alle Quellen, die Sie angeben, werden dann benötigt um die Datenbank zu öffnen. Falls Sie eine Quelle verlieren, kann die Datenbank nicht mehr geöffnet werden.
Master-Passwort:
Passwort wiederholen:
Geschätzte Qualität:
132 Bits
Schlüsseldatei / Provider:
(Keine)
Erstellen...
Durchsuchen...
Eine neue Schlüsseldatei erstellen oder eine existierende auswählen. Falls Sie ein Schlüsselprovider-Plugin installiert haben, ist es ebenfalls in der Combobox aufgelistet.
Windows-Benutzeraccount
Diese Quelle benutzt Daten des aktuellen Windows-Benutzer. Diese Daten ändern sich nicht, wenn das Passwort des Accounts geändert wird.
Falls der Windows-Account gelöscht wird, ist es nicht ausreichend einen neuen Account mit demselben Benutzernamen und Passwort zu erstellen. Ein vollständiges Backup des Benutzeraccounts wird benötigt. Die Erstellung und Wiederherstellung eines solchen Backups ist nicht trivial. Falls Sie nicht wissen wie das geht, lassen Sie die Option deaktiviert.
Hilfe
OK
Abbrechen
www.sicherheit.nw.am

Ist diese erstellt, erscheint links eine Verzeichnisstruktur anhand welcher wir unsere einzelnen Passwörter kategorisiert sichern können.

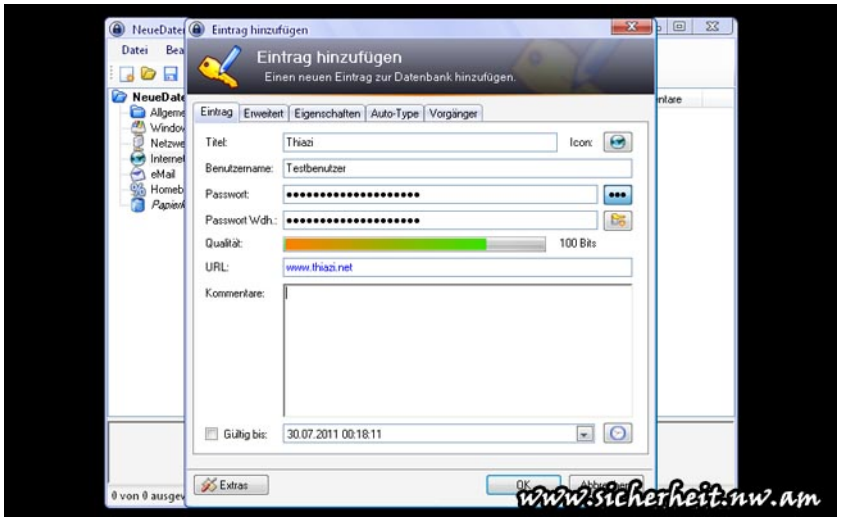
Die beiden Standart Punkte im rechten Fenster können wir ohne bedenken löschen.



Wir suchen uns nun in der linken Verzeichnisstruktur den Punkt aus in dem wir das Passwort gerne speichern möchten und gehen dann auf *Bearbeiten* und *Eintrag hinzufügen*



Im folgenden Fenster können wir nun den Titel des Eintrags, den Benutzernamen sowie das dazugehörige Passwort und eventuell einen Kommentar dazu eingeben. Es ist auch definitiv empfehlenswert, dem Passwort ein Verfallsdatum zu geben, damit man automatisch regelmäßig seine Passwörter ändert. Dadurch kann man sicherstellen, dass von einem Dritten notierte Passwörter ungültig gemacht werden.



Nachdem wir die Felder ausgefüllt haben, bestätigen wir mit ***OK*** und ein neuer Eintrag erscheint nun in unserer Datenbank. Diese Vorgehensweise wiederholen wir nun mit all unseren Passwörtern, welche wir in der Datenbank speichern möchten.

Wichtig ist nur, ein sicheres Haupt-Passwort zu wählen, welches wir auch nicht so schnell vergessen, ansonsten wären ja auch unsere ganzen anderen Passwörter weg. Die Datenbank wird beim Schließen des Programms automatisch wieder verschlüsselt und kann somit bedenkenlos auf der Festplatte oder anderen mobilen Datenträgern gesichert werden.